TUTTO QUELLO CHE GLI ALTRI NON DICONO

2€

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI

n. 177

HACKER JOURNAL

www.hackerjournal.it

LIBERTÀ

SALVIAMO IL NOSTRO BLOG



LINUX

IL PINGUINO DELL'FBI

INTERNET

LA BANDA DI APACHE

TELEFONI PRESIDENZIALI

PRONTO? OBAMA? PRRRRR!!!

QUATTORD. ANNO 9 - N° 177 - 28 MAGGIO/10 GIUGNO 2009 - € 2,00

WLF PUBLISHING

Anno 9 – N.177
28 maggio/10 giugno 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Tempo di cambiare

"Le idee migliori sono proprietà di tutti."
(Seneca)

C'è un momento ben preciso in cui un'idea diffusa diventa "grande", matura, si diffonde, entra a far parte della consapevolezza di molti e inizia a uscire dal substrato sociale in cui è nata, per entrare nella società civile, nel sapere comune. È un passaggio quasi obbligato: le idee si formano in cerchie ristrette di persone e poi passano, diventando spesso ideologie, al resto della popolazione. Se queste idee influiscono sul modo in cui si pensa ai diritti e ai doveri dei cittadini è inevitabile che la trasformazione di queste idee non si esprima in ideologie ma in politica: l'arte di governare.

Per questo motivo, il primo numero realizzato dopo la morte di Fravia, esempio principe di hacker morale, è storico: è anche il primo numero in cui prendiamo atto che, anche in Italia, le idee alla base del movimento hacker, inteso in senso più ampio, si sono trasformate, sono maturate e sono cresciute fino a concretizzarsi in una candidatura politica al Parlamento Europeo.

Sicuramente Fravia non potrebbe che esserne felice: ha combattuto una vita contro l'ideologia di un mercato indifferente alla sorte delle persone, ed è morto proprio nell'anno in cui il Partito Pirata svedese ha acquisito una visibilità mondiale, le Major si trovano al collasso, la questione dei diritti personali sta investendo un'ampia fascia di popolazione e i movimenti underground di tutti i paesi occidentali escono allo scoperto e sfidano i partiti di governo alle elezioni.

Allo stesso tempo, non scordiamolo, questo è il periodo storico in cui le idee circolano nel modo più veloce, si fondono, si trasformano, fanno nascere nuovi movimenti, nuove idee. Noi di HJ, ovviamente, non possiamo far altro che esserne felici e portare il nostro contributo a qualsiasi livello possibile: dalla musica free al miglioramento della sicurezza, dalle notizie che nessuno vuole riportare ai punti di vista inaspettati.

Anche con un ipotetico Partito Pirata Mondiale con un piede in politica, non dimentichiamocelo, siamo hacker: per noi è normale smontare, capire e ricostruire le cose. Così come è normale cambiare completamente il loro utilizzo rispetto a quanto era stato pensato inizialmente. Il tutto, ovviamente, per migliorarle. Per questo motivo non abbasseremo mai la guardia e la nostra informazione sarà sempre libera.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Si sta come d'autunno sugli alberi le foglie



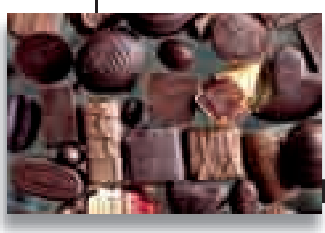
Ma ogniqualvolta possibile è meglio abbandonare i pallidi schermi ed uscire: assaporiamo i crepuscoli a spasso per i centri storici con le nostre compagne, facciamoci accarezzare dal vento e dal sole sulle spiagge, cerchiamo conchiglie con i nostri figli. Ce ne sono di bellissime.

Giuseppe Ungaretti

Non lo conoscevo di persona. Non ho avuto questa fortuna, e per me è un vero rammarico, perché è stato uno di quegli uomini che davvero vale la pena conoscere e frequentare. Ci sono persone molto più adatte di me, amici con cui ho condiviso un'avventura meravigliosa, dai primi insegnamenti di +ORC allo studio del reversing, del software ma soprattutto della realtà, della nostra stessa vita, che possono meglio raccontare chi è stato. Per chi si può fregiare del + della HCU, ma anche per chi non ha avuto modo di partecipare e si è limitato a pescare a piene mani dalla miniera d'oro pubblicata sul suo sito, +Fravia è stato una guida e un ospite meraviglioso, accogliendoci nelle sue pagine così come se ci accogliesse nel salotto di casa, offrendoci conoscenza così come se ci offrisse un drink. Un hacker, a suo modo, ma non nel senso proprio del termine, così come spesso viene inteso. Non passava interminabili ore davanti al monitor per cercare di introdursi in qualche rete, ma per capire e condividere. "Non dare da mangiare all'affamato, ma insegnagli a pescare". Della HCU e del vecchio sito rimane poco in linea, su sua esplicita richiesta, ma ciò che ci ha donato negli ultimi tempi, l'insegnamento su come cercare e trovare quello che si desidera, ha voluto che rimanesse lì, a disposizione di tutti, "perché qui c'è tantissima conoscenza gratuita su come cercare, che aspetta chi tra i visitatori è interessato a imparare e padroneggiare le difficili arti gemelle della ricerca sul Web e del reversing di ciò che si trova" (www.searchlores.org). +Fravia ci ha lasciato domenica 3 maggio 2009, sconfitto da un cancro che ha combattuto fino all'ultimo, ma che gli ha donato anch'esso conoscenza e lo spunto per un nuovo reversing: noi stessi e la vita che abbiamo.

L'AUTO CHE VA A CIOCCOLATO

Si chiama EcoF3 ed è un prototipo di auto da corsa realizzato con le specifiche delle Formula 3, ma a differenza degli altri modelli va... a cioccolato! È il frutto del lavoro dei ricercatori dell'Università di Warwick, in gran Bretagna. Gli studi sull'ecocompatibilità hanno permesso ai tecnici di Warwick di costruire un'automobile che, al posto della classica benzina, utilizza particolari scarti della produzione del cioccolato: il risultato è una velocità massima che tocca i 240 Km/h! Ma il carburante non è il solo elemento ecocompatibile della vettura: il volante ottenuto dalle fibre della carota, il sistema frenante dai gusci di anacardi e molte altre soluzioni tecniche rendono l'EcoF3 biodegradabile al 100%. Insomma, un vero e proprio hack dell'automobile.



SORRIDI, SEI SU INTRUSO-CAMERA

Si tratta di una scena molto comune nei film d'azione e spionaggio: gli investigatori controllano le telecamere di sorveglianza di strade e vicoli per seguire i movimenti dei sospettati di un crimine. A noi tutto questo sembra esagerato ma in realtà l'Italia è uno dei Paesi del mondo più spiati. Con il decreto legge numero 11 del 23 febbraio 2009 infatti, lo Stato autorizza i sindaci dei comuni a installare qualunque sistema di sicurezza atto a monitorare comportamenti sospetti e a garantire la sicurezza dei cittadini. Una cosa ammirevole se non fosse che la privacy di ogni cittadino potrebbe essere violata in qualsiasi momento, senza motivo e soprattutto senza una reale necessità. Il Garante della Privacy infatti si è espresso molte volte su questi sistemi di controllo, limitando i poteri delle amministrazioni per concederlo a chi realmente ha necessità di monitorare i criminali, ovvero le forze dell'ordine. Tuttavia il desiderio di sicurezza ha prevalso sulla libertà d'azione: non sognatevi neanche di non far attraversare un'anziana signora mentre girate in macchina o, ai ragazzi, di disegnare un murale su un vecchio edificio... verreste scoperti e condannati in pochi minuti.



DALLA FONTE DEL P2P
UN FILTRO ANTIPIRATERIA

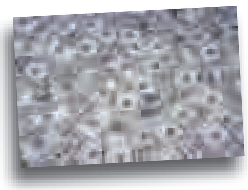
Anche Mininova.org, il popolare Torrent tracker, sarà presto costretto ad adottare un filtro contro la pirateria digitale. Mininova infatti ha deciso di piegarsi alla volontà delle Major cinematografiche dopo che BREIN, l'associazione olandese che difende gli interessi delle industrie discografiche e cinematografiche, gli aveva intimato di non tenere più nel suo database link a file protetti da copyright. Per questo motivo il portale di ricerca di file .torrent si è messo una mano sul cuore e ha accettato la proposta di BREIN: nei prossimi mesi, Mininova proverà alcuni filtri per stabilire quale sia la migliore soluzione tecnica per il sito, dopodiché diventerà quasi impossibile trovare i film in prima visione o gli album appena usciti di band o cantanti. Un peccato? Per i pirati sicuramente sì, tuttavia esistono centinaia di siti come Mininova: vedremo se le Major riusciranno scovarli tutti!





HOT NEWS

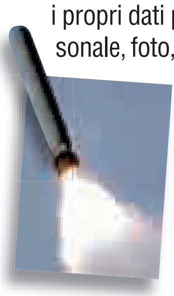
10 MILIONI DI DOLLARI O ADDIO AI VOSTRI DATI



Rischi della Rete, oppure, se volete, il colpo perfetto. Fatto sta che un abile cracker è riuscito a sottrarre dal database della Virginia Department of Health Professions le cartelle cliniche di oltre 8 milioni di pazienti per un totale di 35,5 milioni di prescrizioni mediche. Ma il giovane pirata ha dato un ultimatum (7 giorni) al governo della Virginia per consegnargli 10 milioni di dollari in cambio della restituzione dei documenti rubati. La strategia dell'hacker è stata davvero molto semplice: dopo aver sottratto e criptato tutti i documenti della ASL americana, ha inviato il nuovo file codificato ai legittimi proprietari, ma senza la chiave di accesso. Per avere la chiave quindi lo Stato della Virginia dovrà trovare per tempo i soldi, altrimenti si troverà solo con un po' di byte inutilizzabili in mano. Un riscatto di nuova generazione che va preso sul serio: l'hacker infatti ha minacciato che, in caso di mancato pagamento, utilizzerà le cartelle cliniche dei pazienti nel modo che più gli aggrada, vendendole a società senza scrupoli oppure, perché no, offrendole gratuitamente sul Web.

UN MISSILE ANTINUCLEARE A PORTATA DI MANO

Certe volte la realtà (e la stupidità umana) supera la fantasia. Pochi giorni fa l'FBI ha sottratto a un gruppo di ricerca universitario un PC appartenuto a una struttura di sicurezza in cui erano stati dimenticati i piani segretissimi di un avanzato sistema missilistico antinucleare. A dire il vero il gruppo di ricerca universitaria che aveva acquistato questo computer, insieme ad altri 3 milioni di vecchi PC, voleva proprio testare la sicurezza dei supporti di memoria e la disattenzione degli utenti che vendono i PC usati senza cancellare (o cancellando in modo superficiale) i propri dati personali. Tuttavia i ricercatori si aspettavano di trovare qualche documento personale, foto, video, persino codici di carte di credito o coordinate bancarie (che non sarebbero state utilizzate, trattandosi di una ricerca) ma non avrebbero mai pensato di trovare in un vecchio computer uno scudo antimissile degli Stati Uniti d'America. Dopo l'iniziale sorpresa, la cosa è stata subito segnalata alle autorità federali, che hanno recuperato il computer e i documenti riservati. Tuttavia questo ci insegna a stare molto attenti alle cose che conserviamo sul nostro PC e soprattutto a cancellare accuratamente, con appositi programmi, tutti i nostri documenti prima di venderlo.



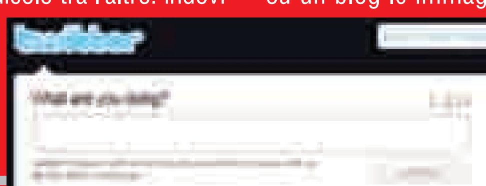
AAA CERCASI HACKERS

Giovane informatico, ottima conoscenza della Rete, con capacità nell'intrusione in sistemi informatici, cercasi. Per informazioni scrivere... al Pentagono! Eh sì, non è una battuta: gli Stati Uniti cercano 250 hacker di alto livello per tenere sotto controllo la Rete alla ricerca di quelle vulnerabilità della sicurezza che spalancherebbero le porte dei sistemi informativi americani a orde di pirati con pessime intenzioni. Il posto di lavoro sarà sicuramente ben retribuito dal momento che gli stipendi di un "anti-hacker" di solito impediscono ai pirati governativi di passare dalla parte del nemico. Del resto i furti informatici sono in crescita esponenziale: Verizon segnala che ogni anno il numero di crimini sul Web è la somma di quello dei quattro anni precedenti. Insomma, 250 hacker potrebbero non bastare a salvare la Rete.



Entra in Twitter... per fortuna senza fare danni

Hacker Croll: questo nome non dice niente a nessuno, neppure voi, o meglio i vostri profili su Twitter, potrebbero essere stati presi di mira proprio da questo brillante pirata. Per segnalare una grossa falla di sicurezza nell'amministrazione dei portale di Twitter, Hacker Croll ha rubato la password di uno degli amministratori del portale (in un modo ridicolo tra l'altro: indovinando la domanda di sicurezza del suo account di Yahoo Mail) ed è riuscito a penetrare nel programma di gestione account di Twitter. Per fortuna si è trattato solo di un'azione dimostrativa che ha portato gli amministratori di Twitter a migliorarne i sistemi di sicurezza interni. Hacker Croll infatti non ha in alcun modo toccato i profili o le informazioni personali dei circa 60 milioni di utenti che ogni giorno visitano il portale. Per dimostrare la veridicità dell'hacking, inoltre, il giovane pirata ha postato su un blog le immagini del tool utilizzato dagli amministratori per gestire le pagine di Twitter. Si tratta comunque dell'ultimo di una serie di problemi di sicurezza che hanno perseguitato il popolare portale di social networking.



RECORD DI ARRESTI

Il 2008 ha fatto segnare un vero e proprio giro di vite per quanto riguarda le truffe online e in particolar modo per la violazione di siti di commercio elettronico mediante la tecnica del phishing. La polizia postale, dopo aver monitorato oltre 12 mila siti Web e aver compiuto circa 600 perquisizioni, ha arrestato 102 persone ree di aver imbrogliato ignari utenti rubando loro le password di accesso a siti di e-commerce con la tecnica del phishing. Il dato più inquietante di questa indagine è però il numero di arresti, 39, per la detenzione e lo scambio di materiale pedopornografico, un numero piccolo ma significativo dei risultati portati dalla Polizia Postale in queste delicatissime operazioni. Inoltre, da pochi giorni, per presidiare meglio la Rete la Polizia Postale ha aperto una sua pagina su Facebook e un canale di Youtube: ecco, se volete scambiarvi qualche file musicale o film con i vostri amici, beh... evitate di girare da quelle parti.



MAC PIÙ SICURO DEL PC?

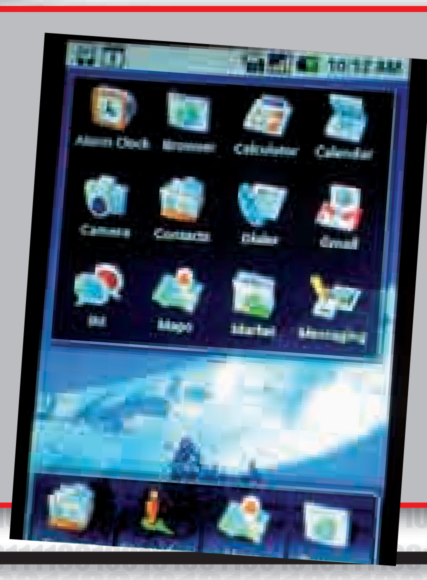
L'immagine che di solito la gente ha di PC e Mac è molto chiara: i PC sono più economici hanno un sacco di programmi ma si piantano più facilmente mentre i Mac, anche se costano una fortuna, sono più affidabili e sicuri. Niente di più sbagliato! A dirlo è il signor Chris Miller, un nome molto famoso negli ambienti hacker, essendo stato per due anni di fila il vincitore del campionato di hacking Pwn2own, nonché il primo essere umano al mondo a craccare l'iPhone di Apple. Secondo Miller, i Mac sono più vulnerabili rispetto ai PC perché non utilizzano tecnologie anti-exploit (ovvero contro i tentativi di aggiramento delle protezioni). Tuttavia, aggiunge però Miller, i Mac sono sempre poco presi di mira dagli hacker: il motivo è che i pirati sono abituati a lavorare bene con i codici di Windows, e sono scoraggiati dai tempi lunghi necessari per creare un exploit per Mac. Infine la bassa diffusione rispetto ai PC di Windows Vista rende l'exploit dei sistemi Apple antieconomico. Insomma, i Mac sono più facili da craccare, ma non conviene: i PC sono molto più diffusi e il bottino è assai più ricco. Che aspettiamo a comprarci un Mac?



DA DELL IL NETBOOK CON ANDROID



Sembra il frutto di un geniale hack: un PC netbook di Dell monta una versione modificata e ottimizzata dell'ormai famoso sistema operativo per smartphone, Google Android. E invece non è così, ma si tratta di una release originale frutto di un accordo commerciale segreto tra Dell, proprietaria dei netbook, e Google, proprietaria del sistema operativo. A rendere pubblica la notizia è stato un prematuro comunicato stampa di Bsquare, partner di Dell nella produzione dei netbook, che per errore è stato inviato alla stampa prima del tempo. La notizia è resa ancora più succosa dal fatto che Dell non ha smentito il contenuto del comunicato stampa, limitandosi a ribadire che l'azienda ha massima attenzione verso le nuove tecnologie. A questo punto ci viene da pensare che non si sia trattato di un errore ma di un'abile mossa di mercato: i netbook si assomigliano un po' tutti e quello di Dell non fa eccezione.





HOT NEWS

I FILE DI WINDOWS 7 ALLARMANO GLI ESPERTI

L'ultima release prima della versione definitiva è uscita da pochi giorni e già gli esperti di sicurezza informatica hanno trovato un bug davvero pericoloso. Ad allarmare la comunità di programmatori, questa volta, è il sistema adottato da Windows 7 per la gestione dei file noti. Windows infatti nasconde l'estensione (ovvero la sigla dopo il punto) di tutti i documenti riconosciuti, come per esempio i file doc di Word, i video in formato avi o le immagini jpeg. Si tratta di un sistema pensato per rendere più rapida la visualizzazione dei file senza avere nella finestra di Esplora Risorse informazioni non necessarie. Tuttavia l'assenza di estensione apre la strada a un semplicissimo trucco. Se infatti vogliamo diffondere un virus (un file eseguibile che normalmente presenta estensione .exe) basterà chiamarlo pippo.doc.exe. Windows, comportandosi come previsto da questa impostazione, nasconderà l'ultima estensione e gli utenti inesperti potrebbero tentare di aprire il file con un doppio clic pensando che si tratti di un normalissimo file di Word. Insomma, è sempre meglio sapere quale tipo di file stiamo per aprire: ogni finestra di Explorer sarà più intasata di informazioni, ma almeno ci risparmieremo la seccatura di essere infettati da qualche virus.



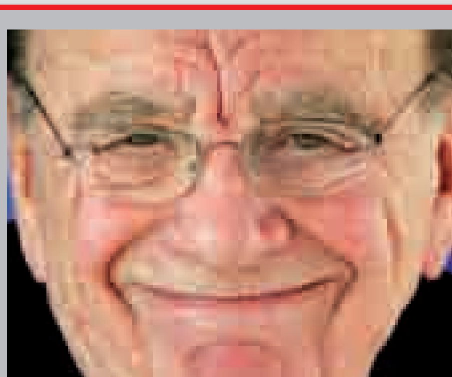
PIRATI SENZA RISPETTO

Nei giorni scorsi è stato rilasciato nei principali negozi online di musica il brano Domani 21/4.2009, una canzone prodotta e interpretata dai più famosi cantanti italiani con l'obiettivo di raccogliere fondi per la ricostruzione delle zone terremotate in Abruzzo. La FMP (la federazione per la lotta alla pirateria musicale) ha però lamentato il cattivo comportamento degli utenti italiani: in oltre 1 milione hanno scaricato illegalmente la canzone dai circuiti del P2P, e se ne trovano versioni facilmente recuperabili anche su Youtube e Facebook. Molti artisti hanno condannato questo atteggiamento contro un'iniziativa che ha senso solo se chi vuole ascoltare la canzone paga il suo contributo all'Abruzzo. Chi è tormentato dai sensi di colpa, può andare sul sito www.domani21aprile2009.it/ e donare 1 euro alle vittime del terremoto.



MURDOCH E L'INFORMAZIONE A PAGAMENTO

Secondo il magnate Rupert Murdoch, padrone tra le altre cose dell'emittente televisiva Sky, il futuro delle notizie in Rete è a pagamento. L'epoca che stiamo vivendo, in cui tutti i portali di news del mondo sono accessibili gratuitamente sta per finire e presto molti importanti giornali nel mondo passeranno a una versione pay. Come già avviene per il Wall Street Journal, presto anche il Sun e il Times saranno disponibili solo a chi stipulerà un abbonamento alla testata. Murdoch ha già in mente il futuro scenario del mondo dell'informazione, in cui le news saranno accessibili a tutti ma gli approfondimenti potranno essere scaricati su appositi e-reader soltanto a pagamento. Fa riflettere che, in un mondo in cui ci sono migliaia di organizzazioni che lottano per la diffusione gratuita di qualunque informazione, sulla Rete ci siano ancora così tante aziende (molte delle quali con decenni di storia alle spalle) che pensano a come poter spillare soldi ai navigatori. A quando il primo giornale piratato?





CHI HA PAURA DEL WEB?

Blog liberi, blog condannati, blog salvati. Blog cattivi o cattivi blog? Dipende

Siamo al 65° posto, in compagnia di Samoa, un gradino sopra il Cile e uno sotto la Nuova Guinea. Stiamo parlando della classifica che Freedom House, organizzazione non governativa che registra il livello di libertà nel mondo, pubblica ogni anno. Il report completo, fino al 2008, è disponibile sul sito dell'organizzazione, freedomhouse.org, e sancisce un record tutto italiano: siamo l'unico Paese d'Europa che costatemente perde posizioni nella classifica che vede svettare Finlandia e Islanda. Se un premier che ha nei Media e nella comunicazione interessi notevoli contribuisce al declassamento, una parte di questo è senz'altro dovuta all'attenzione particolare della politica nei confronti dei nuovi Media, blog in testa.

:: Blog su, blog giù

Già la presenza della legge sulla stampa, che prevede la necessità di iscrivere ad un albo i cittadini che vogliano parlare di determinati argomenti, definendo in modo preciso chi può fare informazione, è un'eccezione nazionale. Quando poi questa legge viene toccata cercando di coinvolgere le fonti di informazione online, in cui la distinzione tra fruitori e fornitori di notizie ha un confine estremamente labile, il rischio è quello di imbavagliare un popolo intero. È quello che è accaduto già nel 2007, quando le modifiche della legge coinvolgevano anche tutti i siti Web, costringendo chiunque tenesse un blog all'iscrizione nel registro degli operatori di comunicazione. In un istante metà del Paese si ritrovava definito dalla legge come editore: dal ragazzino che aveva un blog sulla vita di classe alla casalinga che suggeriva ricette. Chiunque poteva incorrere nei reati a mezzo stampa e chi non si fosse iscritto sarebbe incorso in una denuncia per stampa clandestina. Sull'onda delle proteste, alcuni parlamentari hanno iniziato a dissociarsi fino ad affossare la proposta di legge. Poi, nel 2008, una novità: un'altra legge

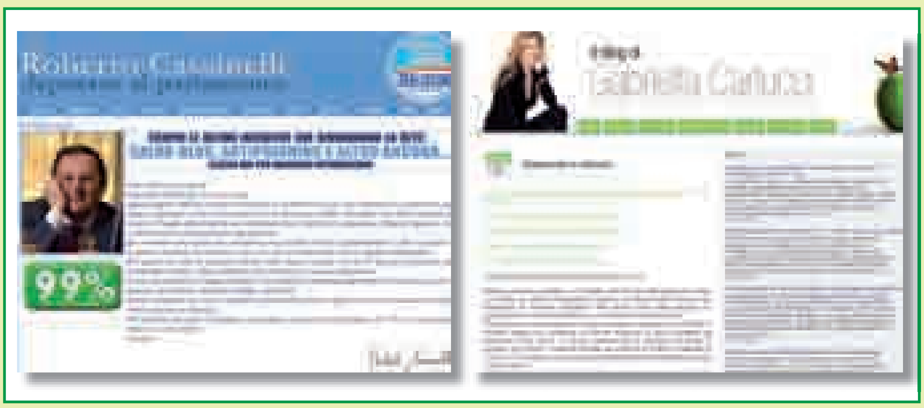
che prevedeva l'inclusione nel ROC (Registro degli Organi di Comunicazione) di chiunque avesse un'entrata economica dalla pubblicazione di un blog, compresi tutti quelli che esponevano banner pubblicitari. Ennesimo moto di proteste, ennesime dissociazioni dei parlamentari, ennesimo affossamento della legge. A un certo punto, alla fine del 2008, l'Onorevole Roberto Cassinelli ha raccolto in una proposta di legge i suggerimenti ricevuti dai bloggers per creare una legge che potesse regolamentare un campo così sensibile. A farsi largo nelle cronache, ormai nel marzo 2009, è spuntata la proposta dell'Onorevole Gabriella Carlucci. Proprio la Carlucci della TV, che ha tirato fuori dalla manica un provvedimento, detto "ammazzarete", che prevedeva il divieto di pubblicazione di contenuti anonimi in qualsiasi forma, coinvolgendo qualsiasi entità presente in Rete (operatori, gestori di siti e piattaforme, utenti) nel rispetto della disciplina, rendendola corresponsabile di ogni genere di reato. Inutile dire che, portato avanti con la scusa della lotta alla pedofilia ma palesemente creato per dare il colpo di grazia alla pirateria informatica, i risvolti liberticidi di questa proposta non hanno fatto altro che spingere ancora di più la proposta di Cassinelli. A questa nuova ondata di sostegno per una legge che tuteli le libertà individuali si è contrapposto l'Onorevole Gianpiero D'Alia, che ha proposto di inserire nel DDL detto "pacchetto di sicurezza" un articolo intitolato "Repressione di attività di apologia o istigazione a delinquere compiuta a mezzo Internet". In perfetto stile Sarkozy proponeva di trasformare gli ISP in poliziotti che dovevano filtrare i contenuti immessi dagli utenti, pena la corresponsabilità nei reati, dando al Governo ampi margini discrezionali di intervento. Una proposta che, per fortuna, è stata bocciata.



Freedom House, freedomhouse.org, è un'associazione non governativa che giudica le libertà concesse negli Stati del mondo. Se fosse un campionato di calcio, sarebbe ora di cambiare l'allenatore.

:: Terrorizzati dai cittadini

Naturalmente, il precedente è solo un tentativo di riassumere una contrapposizione che vede lottare tra loro due gruppi di onorevoli. L'uno che vede in Internet la nemesi storica di ogni Istituzione, il motivo di corruzione dei giovani, di sfascio della nostra società, la base della pirateria, dell'illegalità, della pedofilia; l'altro convinto che le libertà costituzionali riservate ai cittadini siano inviolabili e che vadano garantite anche su Internet. Ognuno può trarre le proprie conclusioni, ma va notato come le proposte del primo schieramento si vedano vittime, con una regolarità disarmante, di azioni di assalto politico da parte di vaste aree dei cittadini interessati. Così come va considerato attentamente l'atteggiamento del secondo gruppo, che usa gli strumenti accusati dal primo per raccogliere indicazioni dagli interessati ed esprimere in proposte di legge delle opinioni che, a quanto pare, sono condivise dalla stragrande maggioranza dei netizen. È una contrapposizione tra imposizioni e libertà che proseguirà ancora per anni e che ci vedrà tutti, prima o poi, coinvolti. È la stessa contrapposizione tra chi usa i social network per ampliare le sue possibilità di lavoro e chi li demonizza come una inutile perdita di tempo, tra chi pensa che il Web equivalga alla pedofilia e gli scienziati che sul Web condividono le loro ricerche, tra chi vede l'eCommerce come uno strumento devastante per i piccoli negozi e chi lo considera come un'opportunità di business di portata immensa.



Pro o contro Internet? I partiti sono spaccati, a riprova di questo ci sono i due atteggiamenti contrapposti di Cassinelli e della Carlucci. Per fortuna, chiunque tuteli le libertà di espressione sul Web vedrà il sostegno dei netizen.



Fuori i robot!

Nuove tecniche per i controlli automatici di registrazione

Come si può fare a distinguere una macchina da un essere umano? La domanda potrebbe sembrare pretestuosa ma è oggi fondamentale in campo informatico. Se fossimo posti davanti a una chat, per esempio, sapremmo fare domande adatte per assicurarci al 100% di avere a che fare con un altro essere umano? Fino a qualche anno fa era impensabile avere dubbi del genere ma i programmi hanno acquisito sempre maggiore complessità e sono arrivati a "comprendere" cose che, in precedenza, erano un affare da fantascienza più che da quotidianità. Basta pensare alle webcam capaci di seguire i volti o, addirittura, di riconoscerli, all'oramai altissima affidabilità dei programmi OCR, all'estrema precisione e velocità dei programmi di riconoscimento vocale e ad altri esempi di questo genere.

:: Il pericolo

Fu un brillante matematico, Alan M. Turing, a ipotizzare per primo un test fondamentale per l'informatica, che da lui prese il nome e che le macchine sarebbero potute diventare "intelligenti" se fossero riuscite a simulare stati discreti (tipici del pensare umano) usando le loro istruzioni a stati finiti (tipicamente binari): un'ipotesi che ha dato vita a una branca dell'informatica (l'intelligenza artificiale) dai risvolti attualissimi e, almeno in parte, impensabili da Turing stesso. Oggi esistono software in grado di superare alcuni test di Turing e di sembrare, quindi, umani a tutti gli effetti. Dal punto di vista del Web, questa capacità risulta tuttavia disastrosa: l'esistenza di programmi in grado di fare iscrizioni massicce a un sito o di bot capaci di tentare infinite combinazioni di nomi utente e password (brute force), spacciandosi per utenti e impiegando frazioni di tempo relativamente brevi, può mettere in seria difficoltà qualsiasi servizio Web (e non solo). Per questo motivo i test di Turing, sempre più complessi, sono stati integrati in diversi siti e vengono comunemente chiamati CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart (test di Turing pubblico completamente automatico per distinguere tra umani e computer).

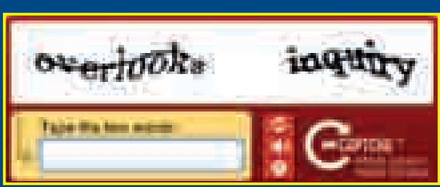
La tecnica oggi più utilizzata per fare questo test consiste nel mostrare alcuni caratteri volutamente offuscati da righe, barre e disegni oppure in modo distorto: un essere umano può comunque leggere ciò che viene scritto e trascriverlo correttamente in una casella, mentre il livello di riconoscimento dei testi da parte di un software non è ancora sufficiente per farlo. In realtà, la parola chiave è "ancora": la velocità di evoluzione dei software e le capacità computazionali degli elaboratori sono in crescita vertiginosa e già oggi i software sono arrivati a un livello sufficiente per passare i CAPTCHA più banali.



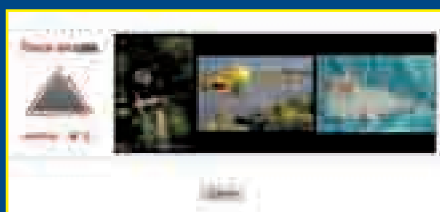
I nuovi CAPTCHA per ora sono solo sulla carta, ma presto potremmo trovarli in uso, a partire dall'accesso di Google che ha già pronto ciò che serve.

:: Ai ripari!

Per questo motivo, Google ha sostenuto un interessante studio sulla possibilità di eliminare i CAPTCHA basati su testo in favore di quelli basati su immagini, con il risultato di eliminare anche le barriere linguistiche alla base dei sistemi attuali e aumentare i successi da parte degli umani, eliminando drasticamente quelli dei bot. Il trucco usato è quello di prendere una grande quantità di immagini di vario genere, eliminando quelle in cui l'orientamento non è perfettamente comprensibile all'uomo. Poi, il sito provvede a mostrare all'utente un'immagine random, ruotandola casualmente. All'utilizzatore è richiesto, tramite controlli in pagina, di ruotare l'immagine fino a porla con l'orientamento corretto. Una volta terminato l'orientamento e ricevuto lo spostamento indicato dall'utente, il sito lo confronta con il valore casuale iniziale, calcola una percentuale di errore (perché, appunto, errare è umano) e, in caso di rotazione corretta, provvede a garantire l'accesso. Tecnicamente, considerando un errore di un grado, ci sono 3 possibilità su 360 di entrare nel sito e un bot potrebbe comunque andare per tentativi. A inficiare ogni attacco, però, è che il nuovo CAPTCHA visuale cambia ogni volta che viene tentato un accesso, modificando il valore da trovare. Se si riduce il margine d'errore ammesso, vengono moltiplicati a dismisura i valori ammissibili, a patto di selezionare con accuratezza le immagini da mostrare. Alcune immagini, infatti, possono essere collocate in diverse posizioni e bisogna evitare assolutamente che un umano possa avere dubbi. D'altra parte non bisogna usare immagini troppo simili tra loro: se si usassero solo immagini di paesaggi, con il cielo blu in alto e l'erba verde in basso, nessun umano sbaglierebbe ma sarebbe anche banale programmare un bot che analizzi l'immagine. Con un gran numero di immagini, di genere molto vario, sarebbe invece possibile realizzare un sistema decisamente più sicuro dell'attuale.



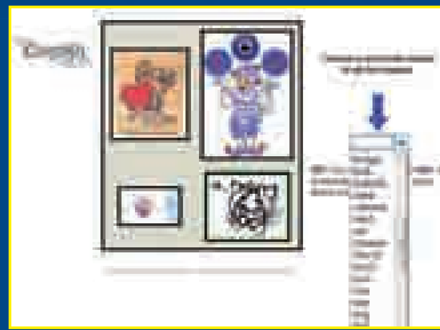
Il classico CAPTCHA è basato su testi distorti che vanno interpretati e riscritti. Purtroppo sbagliano anche gli umani!



CAPTCHA visuali esistono già ma sono basati sul "semplice" riconoscimento di forme e oggetti. Un livello a cui il software è già arrivato.

:: Più semplice, più veloce

Diversamente dai sistemi usati attualmente, il nuovo CAPTCHA ha il vantaggio di non richiedere la conoscenza dell'alfabeto. Un vantaggio che può far sorridere ma che si rivela di enorme importanza pensando a lingue che non sono basate sui caratteri occidentali: russo, arabo, ebraico, cinese, giapponese, eccetera. In più, diversamente dai sistemi attualmente utilizzati, quello basato sulle immagini è facilmente superabile dagli esseri umani. I CAPTCHA tradizionali, infatti, chiedono di riscrivere correttamente alcuni caratteri mostrati in modo confuso, per evitare un riconoscimento automatico OCR, ma le modifiche subite dai testi possono arrivare al punto da essere difficilmente comprensibili anche per gli umani! In un mondo (il Web) in cui un clic in più con il mouse viene attentamente valutato dai proprietari dei siti perché potrebbe scoraggiare gli utenti, la presenza di un sistema di sicurezza che obbliga gli stessi utenti a compilare più volte lo stesso modulo rende vano qualsiasi studio di usability. Grazie al CAPTCHA basato sulla rotazione delle immagini, il problema viene brillantemente superato. Di contro, diversi bot sono in grado di riconoscere gli oggetti o identificare paesaggi ma nessuno è ancora lontanamente in grado di comprendere il contenuto di quello che riconosce. Non avendo alcuna coscienza o backgroud di esperienze, nessun software sarà in grado, per anni, di riconoscere il corretto orientamento di un oggetto. L'unica strada possibile per craccare questo CAPTCHA sarebbe un confronto con le immagini originali: piuttosto difficile se il database delle foto contiene migliaia e migliaia di figure che verranno proposte agli utenti con orientamenti casuali. Il semplice lavoro di riorientare tutte le immagini acquisite da sistemi automatici, da svolgere manualmente, potrebbe portar via diversi anni-uomo di lavoro.



Un CAPTCHA basato su concetti astratti: bisogna riconoscere il concetto comune a 4 immagini. Ma c'è il problema della lingua e di capire i concetti.

L'interessante studio è disponibile come documento PDF all'indirizzo www.richgossweiler.com/projects/rotcaptcha/rotcaptcha.pdf. Restiamo in attesa del momento in cui verrà implementato nei maggiori siti Web.



Anche l'Italia ha un Partito Pirata e un candidato per le elezioni europee: la sveglia è suonata!

Pirati in parlamento!

Negli ultimi tempi la filosofia alla base dei movimenti underground in ambito informatico, di cui diamo in ogni numero ampia rassegna, si sta sempre più concretizzando in impegno politico. È un passaggio necessario, naturale e conseguente: le idee, se influiscono su un modello sociale, devono diventare politiche. Con questa accezione intendiamo quella slegata dal dibattere di veline e divorzi tipicamente italiana: la politica vera, quella del governo delle persone, dal greco Polis. Attenzione: non siamo e non diventeremo mai un giornale di partito o un giornale politico: è contrario alla nostra natura. Il mondo dell'open, dell'hacking, della pirateria intesa come dialettica verso posizioni fossili e antiquate proposte dalle Major, però, ha subito un'evoluzione che lo sta portando in una sfera politica e non possiamo nasconderci dietro a un dito.

Lo sa bene la Svezia, dove il Partito Pirata è ormai tra i maggiori partiti politici e si è fatto portavoce di una richiesta di libertà che già da anni permeava la loro società civile. Per questi motivi siamo felici di annunciare che anche nel nostro Paese questo movimento di idee si sta trasformando, concretizzandosi in una formazione politica.

:: Anche in Italia

Si chiama Alessandro Bottoni, è un consulente informatico, ha 48 anni, nel 2006 ha fondato il blog La Spina nel Fianco (laspinanelfianco.wordpress.com) in cui metteva in guardia verso le tecnologie di Trusted Computing e, nel 2006, ha fondato insieme ad Athos Gualazzi, Daniele Masini ed altri il Partito Pirata Italiano. Lo scopo è quello, comune e condiviso da moltissimi cittadini, di chi conduce una battaglia alla luce del Sole contro gli interessi economici delle lobby: promuovere una riforma liberista della legge sul diritto d'autore. Dal punto di vista politico è un vecchio comunista, militante nella FGCI e nel PCI. A differenza di altri, però, gli è capitata l'occasione di rendere ancora più esplicita la sua battaglia per la libertà, condotta inizialmente all'interno di formazioni politiche già esistenti, con l'adesione alla lista Sinistra e Libertà, nella circoscrizione 2 Nord/Est (nelle regioni Emilia Romagna, Veneto, Friuli Venezia Giulia e Trentino-Alto Adige).

PARTITO-PIRATA

:: HJ che c'entra?

Abbiamo deciso di parlare proprio di lui perché, al di là del colore politico del candidato e della lista,



Il sito del Partito Pirata Italiano, www.partito-pirata.it, organizzazione non governativa che promuove in modo nuovo il diritto d'autore.

è facile capire come gli impegni siano comuni e perfettamente allineati. Lo stesso Bottoni anticipa ogni possibile recriminazione firmando una lista di impegni che si porterà al Parlamento Europeo in caso di elezione: dalla competenza tecnica (di cui si nota l'estrema carenza da parte di molti altri politici) fino alla promessa di introdurre nelle commissioni le idee di libertà individuale che spesso sono state calpestate dalle norme vigenti. Con la novità di impegnarsi a portare fuori dalle commissioni, dandone visibilità sui blog, quelle discussioni che potrebbero smascherare i molti interessi economici dietro decisioni prese con la "scusa" della convivenza civile e degli interessi nazionali. La sua iscrizione in una lista non dedicata esclusivamente al Partito Pirata, accusa che gli si potrebbe rivolgere, è stata un passaggio pressoché obbligato: la Legge 10 del 20 febbraio 2009 ha introdotto uno sbarramento al 4% per potersi presentare alle elezioni. Da solo non avrebbe avuto le firme necessarie alla candidatura, problema che con una lista comune ad altre persone con idee comunque simili ha potuto superare. Ora, però, non bisogna perdere l'occasione: al Parlamento Europeo saranno quasi sicuramente presenti altri membri dei partiti pirata di altre nazioni, in primis quello svedese. Questo significa che un'azione congiunta da parte di questi ospiti, ovviamente indesiderati dai politici tradizionali, potrebbe rimettere in equilibrio la bilancia di diritti e doveri dei cittadini dal punto di vista legale. Finalmente si potrebbe impedire non solo che degli intermediari si prendano la più grande fetta di profitti economici, ma si profilerebbe l'eliminazione di quelle leggi che bloccano l'iniziativa personale, impedendo la libera circolazione delle idee e limitando le libertà personali.



Sul suo blog personale, Bottoni, non parla solo della sua candidatura, ma anche di diritti, tecnologia e pericoli.



Sul blog de Il Progetto Arancione si trovano tutte le notizie riguardanti la candidatura: dalle iniziative intraprese a informazioni sul suo passato.

:: Un impegno serio e trasparente

Diversamente da altri candidati, riciclati o trasformisti dell'ultima ora, Alessandro Bottoni, proprio grazie alla Rete e alla sua conoscenza delle tecnologie informatiche è totalmente trasparente. Basta una ricerca su Google per trovare pro e contro della sua candidatura, per sapere molte cose su di lui, per ottenere informazioni provenienti da fonti diverse. Lui stesso sta usando il Web per portare avanti la propria candidatura e per informare tutti gli interessati del suo "Progetto arancione"; basta leggere il suo blog personale, alessandrobottoni.wordpress.com, oppure il sito dedicato al progetto: ilprogettoarancione.wordpress.com per rendersene conto.

IMPEGNI TRASPARENTI

Contrariamente a molti altri candidati, di cui non si sa che impegni si siano presi o come la pensino su molte cose, **Alessandro Bottoni** ha l'onestà e la forza di rendersi completamente trasparente ai suoi possibili elettori.



Ovviamente in Rete:

- **ilprogettoarancione.wordpress.com/whoami**
  Una autobiografia dettagliata.
- **alessandrobottoni.wordpress.com**
  Il suo blog personale, aggiornato quotidianamente.
- **ilprogettoarancione.wordpress.com/impegno-per-la-scienza-e-la-tecnologia**
  L'impegno, di ampia portata, per aumentare le possibilità offerte alla crescita scientifica.
- **alessandrobottoni.wordpress.com/contacts**
  Tutti i metodi per contattarlo personalmente: dalla mail personale agli SMS. Una vera novità nel panorama nazionale, composto in molti altri casi da risposte preconfezionate da anonimi addetti stampa.

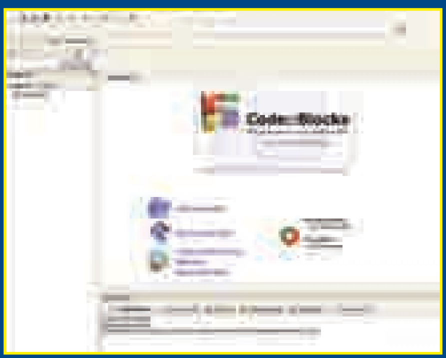
FREE È MEGLIO!

Se vogliamo imparare a programmare, un IDE come Code::Blocks fa proprio al caso nostro

Torniamo a parlare di ambienti di sviluppo per presentare Code::Blocks, un IDE che non mancherà di meravigliarci per la pulizia dell'interfaccia e la facilità d'uso. Si tratta di un progetto Open Source, disponibile per molti sistemi operativi ed è estremamente versatile: basa la propria architettura su un sistema a plugin, per cui è molto facile personalizzarlo secondo le nostre esigenze. In più, supporta numerosi compilatori ed è compatibile con i progetti creati in Dev-C++ e con il suo sistema di DevPak per la distribuzione di librerie.

:: Download e installazione

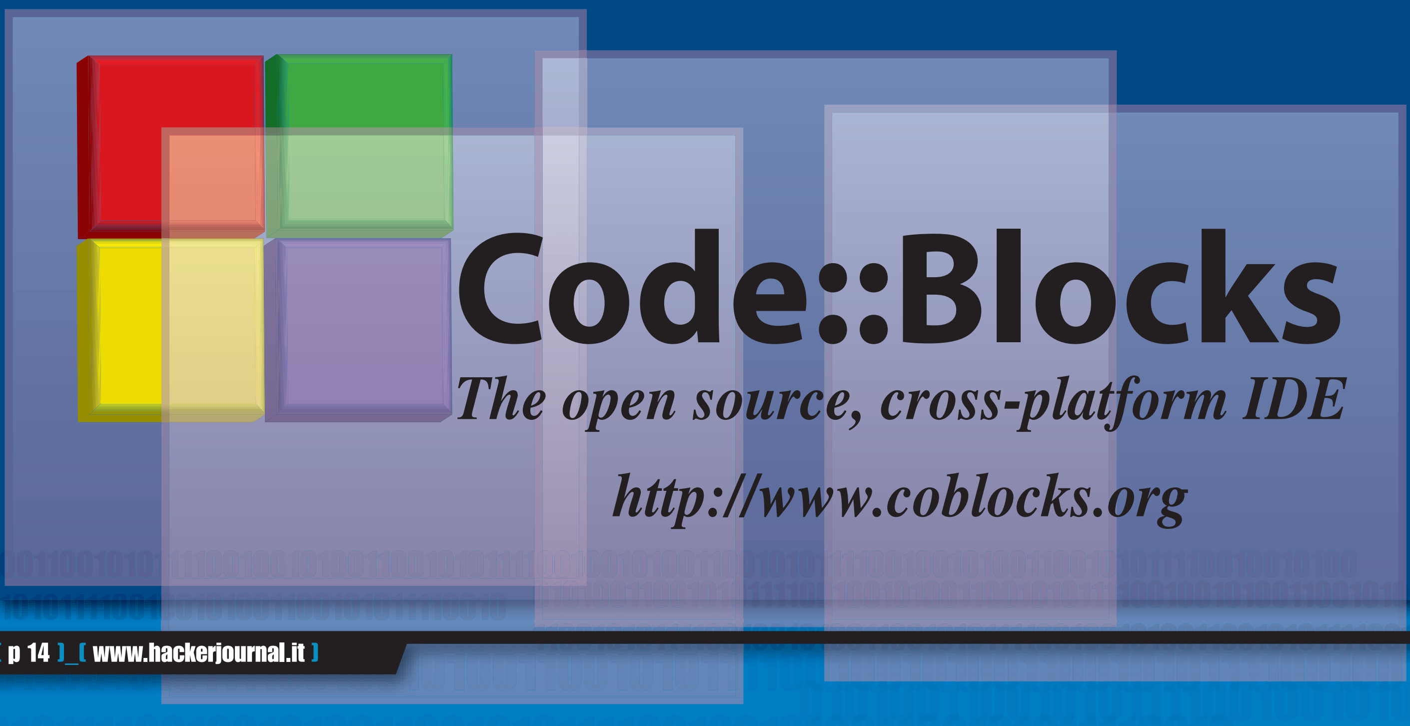
Il sito ufficiale di Code::Blocks è all'indirizzo http://www.codeblocks.org e ci consente di scaricare gratuitamente il programma e le guide all'uso, disponibili però solo in inglese e tedesco, nei formati HTML, PDF e CHM. Tra i download sono disponibili i file binari (eseguibili) per diversi sistemi operativi, tra i quali Windows, MacOS X e Linux, i sorgenti della versione stabile e, per chi vuole magari partecipare allo sviluppo dell'applicazione, la versione SVN, che mette a disposizione l'ultimissima release in lavorazione, comprendente gli ultimi bugfix al momento in cui vengono rilasciati. L'installazione non comporta alcun problema: basta lanciare l'eseguibile scaricato da Sourceforge.net o da BerliOS.de e la solita procedura guidata ci aiuta a configurare il programma sul nostro computer. Durante il processo, possiamo scegliere quali plugin vogliamo installare e quali moduli (Lexers) per il code highlighting, che migliorano la leggibilità del codice colorando diversamente gli elementi che lo compongono. Se sappiamo già per cosa useremo Code::Blocks, possiamo limitarci a installare solo i plugin e i lexers che ci sono più utili, ma se non ne siamo ancora sicuri non è un problema installarli tutti.

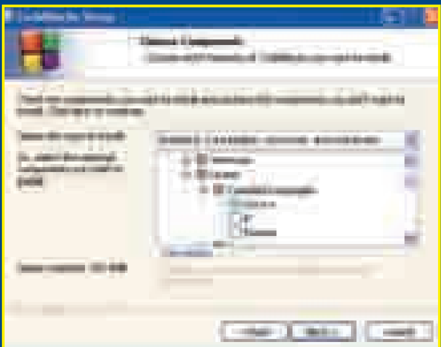


L'interfaccia principale è divisa in pannelli che forniscono strumenti e informazioni sul lavoro in corso.

:: L'interfaccia

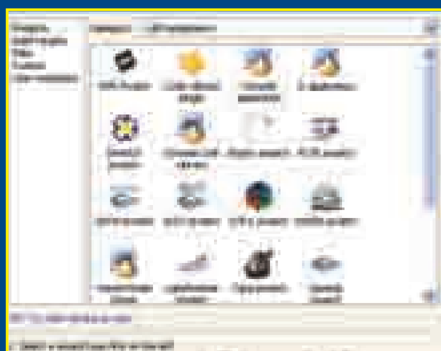
Al primo avvio, Code::Blocks effettua una scansione del sistema per cercare i compilatori ricono-



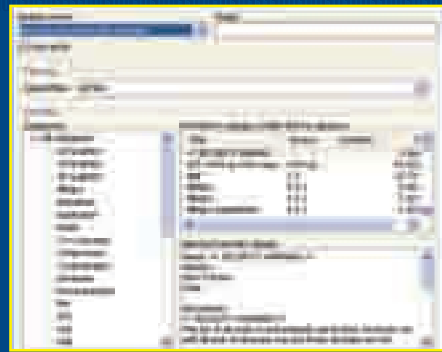


Durante l'installazione possiamo scegliere i plugin e i moduli da includere secondo le nostre esigenze.

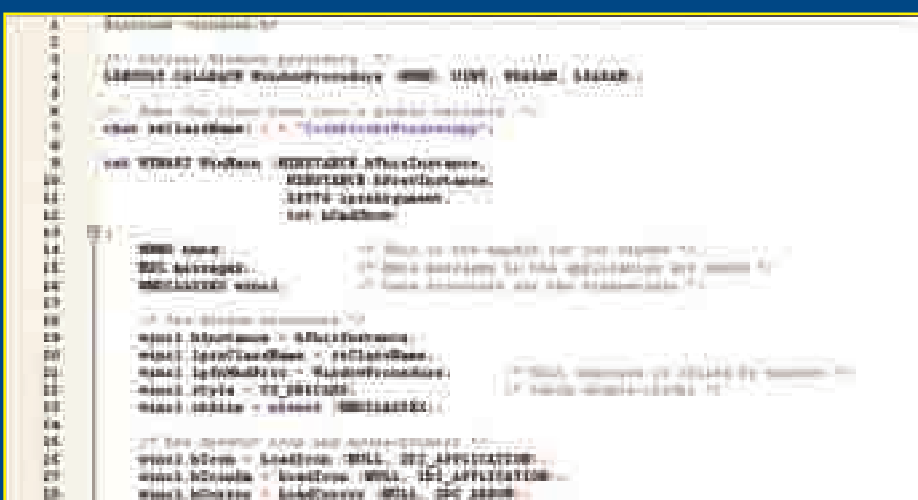
sciuti eventualmente installati: il programma è distribuito con MinGW ma supporta numerosi altri compilatori. Se ne abbiamo uno preferito già installato nel sistema e vogliamo adottarlo come predefinito al posto di MinGW, ci basta selezionarlo e fare clic sul pulsante Set as default e poi su OK. Si avvia quindi l'interfaccia principale, che mostra un "Tip of the Day" e ci dà la possibilità di associare Code::Blocks con i file di tipo C/C++, in modo che basti fare doppio clic sulla loro icona per aprirli con il programma.
Dalla schermata principale, come è ormai prassi per tutti gli ambienti di sviluppo integrati, possiamo aprire un progetto esistente o crearne uno nuovo. I tipi di progetto che sono a nostra disposizione, basati su template, dipendono dai moduli che abbiamo installato. Col tempo, aggiungendo nuovi moduli e nuove librerie, sono destinati a crescere, soprattutto se sfrutteremo a fondo la compatibilità di Code::Blocks con Dev-C++. Importando i DevPak di quest'ultimo, infatti, li avremo automaticamente a disposizione come ulteriori tipi di applicazione per avere sempre pronta la struttura di base dei nostri nuovi progetti. La creazione di un nuovo progetto avviene mediante procedura guidata. Il numero di passaggi e le operazioni compiute in questa fase variano in base al tipo di progetto scelto. Al termine della procedura, avremo creato sul disco le cartelle contenenti tutti i file che compongono il progetto e nella finestra principale di Code::Blocks potremo aprire il file sorgente che contiene lo scheletro della nostra applicazione. Nella finestra principale avremo a nostra disposizione non solo un comodo editor con syntax highlighting per scrivere il nostro codice, ma una vera e propria centrale di controllo con cui possiamo compiere compilazioni di diverso tipo (per esempio Release o Debug) ed effettuare il debug dell'applicazione in corso d'opera.



I tipi di applicazione che si possono creare sono numerosi e dipendono dalle librerie e dai plugin installati.



L'importazione e l'installazione dei DevPak di Dev-C++ è facilitata dalla presenza di un apposito plugin.



Una volta creato il progetto con la relativa procedura guidata proposta da Code::Blocks, possiamo aprire nell'editor i file con il sorgente e iniziare a lavorare per aggiungere il codice che ci serve per far funzionare la nostra applicazione.

:: Espandibilità

Come accennato all'inizio di questo articolo, Code::Blocks è in grado di "digerire" librerie di espansione di vario genere, tra cui quelle sviluppate per Dev-C++ in formato .devpak (posto che abbiamo installato l'apposito plugin in fase di setup). Questa possibilità è molto comoda, in quanto le librerie in questione sono numerose, spesso costantemente aggiornate, e possono risolvere molti problemi di programmazione. Troviamo il comando Dev-C++ DevPak update/installer nel menu Plugins: selezionandolo viene mostrata la finestra di dialogo che ci permette il collegamento al repository dei pacchetti e di scaricare e installare quelli che desideriamo. Selezionando invece Manage plugins potremo gestire con un'unica finestra anche tutti gli altri moduli di espansione, che vengono distribuiti sotto forma di file con estensione .cbplugin. Molti sono già presenti con l'installazione del programma, ma trovandone di nuovi, basterà scaricarli e installarli nel programma con questo strumento. Allo stesso modo è possibile includere più compilatori da usare nello stesso ambiente di sviluppo. Questa possibilità è utile quando si devono compilare software per piattaforme diverse, per esempio usando un cross-compiler che crea codice per sistemi embedded. Con il comando Settings → Compiler and debugger possiamo impostare il compilatore da usare con i relativi parametri.



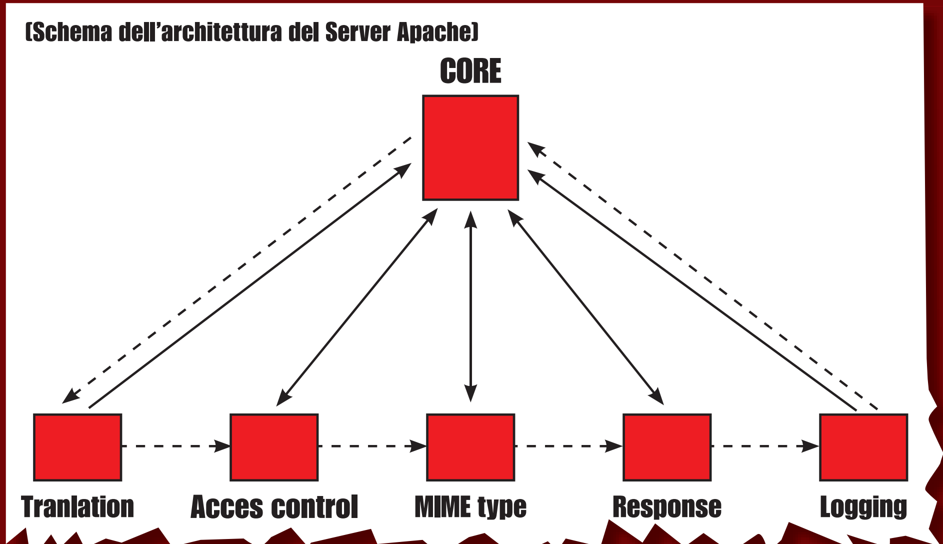
Configuriamo Apache per rispondere alle nostre esigenze

LA BANDA DI APACHE

Apache è senza dubbio il server Web Open Source più famoso e più utilizzato al mondo. Fin dalla sua nascita nel 1995 gli sviluppatori hanno incentrato i propri sforzi per creare un sistema dotato di buone performance, strutturato in maniera modulare e compatibile con la maggior parte delle architetture hardware esistenti. Queste caratteristiche, insieme alla facilità di configurazione, lo hanno portato ad essere utilizzato, ad oggi, in oltre il 45.95% dei server al mondo (bollettino "April 2009 Web Server Survey" di NetCraft.com). In questo articolo andremo ad analizzare come è possibile gestire la banda a nostra disposizione sfruttando alcuni moduli di Apache.

:: Problema

Da quando esiste il World Wide Web è pratica comune ospitare diversi siti Internet su un solo server Web. Per non ricorrere alla virtualizzazione e per non acquistare un indirizzo IP dedicato per ogni sito in host sulla macchina, la maggior parte dei sistemisti ricorre all'uso dei Name VirtualHost. L'utilizzo di questa funzionalità è una scelta economicamente vantaggiosa e



[Codice 1]

```
sudo apt-get update // per aggiornare la lista dei pacchetti del sistema all'ultima versione disponibile
sudo apt-get install apache2 // per avviare l'installazione vera e propria di Apache
```

[Codice 2]

```
<VirtualHost *:80 >
ServerAdmin webmaster@nomedominio.it
ServerName www.nomedominio.it
DocumentRoot /var/www/nomedominio.it/public
</VirtualHost>
```

proficua, visto che in questo modo viene limitata l'infrastruttura hardware (meno server = meno costi) e la sua relativa gestione (meno server = meno sistemisti) per la compagnia di hosting. Il problema che si verifica in buona parte delle aziende però è la presenza di troppi siti Web sullo stesso server. Tante compagnie ospitano infatti migliaia e migliaia di siti Internet su un unico server per massimizzare i propri ricavi, non curandosi del calo delle prestazioni che una politica di questo tipo può creare. Prendiamo in considerazione i due estremi: andrà più veloce un sito Internet in host su una macchina totalmente dedicata o un sito Internet che condivide le risorse del server (banda a disposizione, RAM, CPU, eccetera) con mille altri? Nel corso degli anni, grazie anche a numerose compagnie che attuavano in maniera selvaggia questa politica, gli utenti hanno iniziato a chiedere una garanzia sui livelli prestazionali offerti dall'azienda, quali appunto banda dedicata, CPU dedicata, RAM dedicata e altri parametri. Questo tipo di contratto viene ad oggi definito "Service Level Agreement", più comunemente chiamato "SLA", e viene oramai integrato nei contratti standard dalla maggior parte compagnie del settore. Ma a livello di configurazione, come è possibile implementare una frammentazione della banda su più siti Web?

:: Installazione di Apache

Per iniziare i nostri test occorre innanzitutto installare Apache (oggi disponibile per il download la versione 2.2.11) rilasciata sia per sistemi Unix che per Win32. In questo articolo verrà utilizzata una configurazione con sistema operativo Debian GNU/Linux. Da riga di comando, digitiamo le stringhe di **Codice 1**. Già fatto? Ebbene si, se non volete cambiare la configurazione di default, il vostro server Web è già pronto e operativo. Se invece volete darvi alle configurazioni vi rimando al file dedicato presente di default in /etc/apache2/apache2.conf. Prima di passare ai VirtualHost è bene sottolineare come nel mondo dei computer sia possibile configurare un sistema per effettuare la medesima operazione in modi diversi. Il famoso detto "tutte le strade portano a Roma" è infatti anche valido nell'ambito informatico. Di seguito analizzeremo una delle tante tipologie di configurazione, sta a voi decidere se è la migliore, la più semplice o, comunque, quella più adatta alle vostre esigenze operative.

:: Configurazione VirtualHost

Di default la DocumentRoot (ovvero la directory dove risiedono i file veri e propri del sito Web) in un sistema Linux è /var/www/. Creiamo quindi una directory al suo interno per ogni sito Internet che vogliamo ospitare utilizzando il comando:

```
mkdir /var/www/nomedominio.it
```

e creando all'interno di essa altre due cartelle dal nome public e cgi-bin. La prima sarà la cartella pubblica dove risiederanno gli script, le immagini e le cartelle del sito Web, la seconda servirà per l'utilizzo di eventuali script CGI da utilizzare. Dopo aver fatto ciò andiamo a creare il file di configurazione del dominio dove scriveremo i parametri del VirtualHost:

```
nano /etc/apache2/sites-available/nomedominio.it
```

Al suo interno inseriamo un testo simile a quello descritto in **Codice 2.** Analizzando questa semplice configurazione possiamo notare che tutte le connessioni in ingresso sulla porta 80 del server verranno indirizzate al sito Web presente nella directory /var/www/nomedominio.it/public grazie alla condizione <VirtualHost *:80 >. Vediamo ora come configurare la larghezza di banda dedicata ad ogni singolo VirtualHost presente nel sistema. Per fare ciò possiamo utilizzare tre diverse soluzioni.

:: 1) mod_cband

È un modulo di Apache dotato anche di interfaccia Web che



Lo screenshot del pannello di controllo relativo al modulo CBAND.

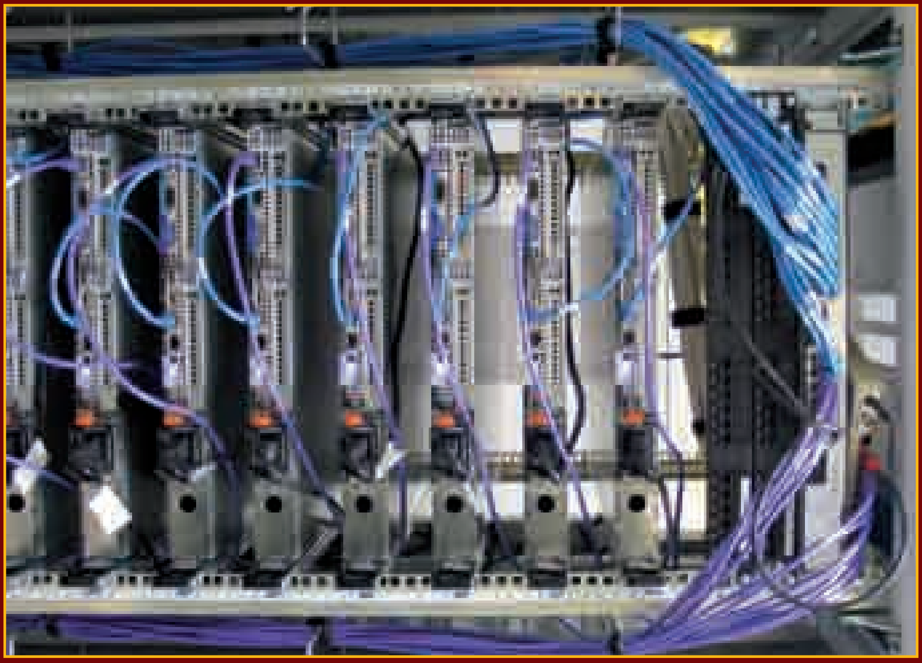


L'interno di un server Dell PowerEdge 850 utilizzato come Web server.

ci permette di visualizzare e gestire in maniera completamente user friendly le limitazioni di banda per ogni singolo VirtualHost. In alcune distribuzioni questo modulo dovrebbe già essere installato di default con Apache e necessita solo di essere abilitato nel file di configurazione /etc/apache2/apache2.conf aggiungendo (o togliendo # dalla linea) LoadModule cband_module modules/mod_cband.so. Nel caso che comunque non fosse ancora installato ci basta un colpo di apt-get da terminale per farlo:

```
apt-get install libapache2-mod-cband
```

(se non fossero ancora installati bisogna soddisfare le dipendenze installando anche i pacchetti apache2-utils e apache2-threaded-dev).



I cablaggi del Rack Server di Wikipedia, ubicato ad Amsterdam.

Non ci resta che inserire le righe:

```
CBandScoreFlushPeriod 1
CBandRandomPulse On
```

all'interno del file di configurazione/etc/apache2/httpd.conf, riavviare il demone Apache con un bel /etc/init.d/apache2 restart e creare la directory scoreboard con il comando:

```
mkdir /var/www/scoreboard
chown www-data:www-data /var/www/scoreboard/
```

A questo punto il modulo è correttamente installato e pronto all'uso, non resta che aggiungere le limitazioni per i VirtualHost come di seguito:

```
CBandSpeed 1024 10 30
CBandRemoteSpeed 20kb/s 3 3
```

La direttiva CbandSpeed limita le performance totali di Apache per quel singolo VirtualHost a una velocità massima di 1024 Kbps, con un massimo di 10 richieste al secondo e di 30 connessioni aperte. La direttiva CbandRemoteSpeed è simile alla precendente ma serve a limitare le performance per ogni singolo utente. Ci sono poi altre direttive come CbandLimit, CbandScoreboard, CbandDefaultExceededCode, CBandDefaultExceededURL che lasciamo a voi approfondire. È possibile poi, grazie alla comoda interfaccia Web presente all'indirizzo http://INDIRIZZOIP/cband-status/, visualizzare in maniera grafica l'utilizzo e la ripartizione della banda in tempo reale.

Ricordiamoci che alla fine di ogni variazione ai file di configurazione è necessario riavviare Apache per rendere operative le modifiche effettuate.

:: 2) mod_bandwith

Questo modulo è parecchio simile, sia come installazione che come configurazione, a mod_cband, ma permette di impostare in maniera più professionale i parametri limite per ogni VirtualHost. Non dobbiamo neanche procedere ad alcun tipo di setup in quanto il modulo è già presente di default nell'installazione di Apache. L'unica cosa che dobbiamo

```
[Codice 3]
# mkdir /tmp/apachebw
# mkdir /tmp/apachebw/master
# mkdir /tmp/apachebw/link
# chown -R www-data:www-data /
tmp/apachebw
# chmod -R 775 /tmp/apachebw
```

fare per abilitarlo è controllare che all'interno del file /etc/apache/modules.conf sia presente e non sia commentata (con un #) la riga LoadModule bandwidth_module /usr/lib/apache/1.3/mod_bandwidth.so.
Creiamo due directory con i comandi riportati in **Codice 3** e riavviamo Apache per rendere operative le modifiche utilizzando il comando /etc/init.d/apache2 restart.

A questo punto non ci resta che impostare le limitazioni di banda sui vari VirtualHost di sistema. Per fare ciò questo modulo ci mette a disposizione molteplici direttive. Andiamo ad analizzare le più importanti.

- **BandWidthModule**: è la direttiva più importante e permette di abilitare (con ON) o disabilitare (con OFF) il funzionamento del modulo in maniera selettiva per ogni VirtualHost.
- **BandWidthDataDir**: imposta la directory in cui mod_bandwidth conserva i suoi file temporanei (nel nostro caso dobbiamo settare come directory la path /tmp/apachebw che abbiamo creato precedentemente).
- **BandWidthPulse**: specificando un valore temporale, espresso in millisecondi, permette al modulo di variare l'algoritmo con cui vengono trasmessi i dati durante tale periodo.
- **BandWidth**: limita la banda per i file contenuti nella directory e nelle subdirectory, in base alla provenienza (prendendo in esame nome dominio, indirizzo IP o entrambi).
- **LargeFileLimit**: imposta una diversa disponibilità di banda in base alla grandezza dei file che si condividono (veramente utile nel caso di siti molto trafficati che permettono il download di file di grandi dimensioni).
- **MaxConnection**: permette di specificare il numero massimo di connessioni simultanee oltre il quale il nostro server risponde con un rifiuto. Di default (se non specificato in maniera diversa) questo valore è impostato su 0 (infinite connessioni simultanee).
- **MinBandWidth**: a mio avviso una delle più importanti direttive che ci mette a disposizione mod_bandwith. Permette infatti di impostare una banda minima garantita assegnata per ogni VirtualHost (tornando al discorso iniziale: è grazie a questa direttiva e a molti altri fattori che possiamo garantire una SLA per ogni dominio).

:: 3) mod_iptos

È una particolare soluzione alternativa che, a differenza delle precedenti, non si occupa di gestire la quantità di banda ripartendola per ogni VirtualHost, ma la sua qualità, grazie a quattro differenti Type of Service (TOS): lowdelay, throughput, reliability, lowcost.
Per la configurazione vi consigliamo di scaricare e installare il pacchetto direttamente dal sito ufficiale (http://arctic.org/~dean/mod_iptos/) e, come nei casi precedenti, controllare che il modulo sia debitamente abilitato e decommentato all'interno del file /etc/apache/modules.conf. Qui di seguito trovate alcuni diversi tipi di impostazione riguardanti questo modulo (**Codice 4**).
Vista però la particolarità di configurazione dello stesso in base alle proprie esigenze di servizio vi rimandiamo al sito Internet ufficiale per ottenere ulteriori informazioni a riguardo.

```
[Codice 4]
# default to IPTOS none, but files
larger than 5MB are marked
# throughput
IPTOS none
IPTOSthreshold 5000000
throuhgput

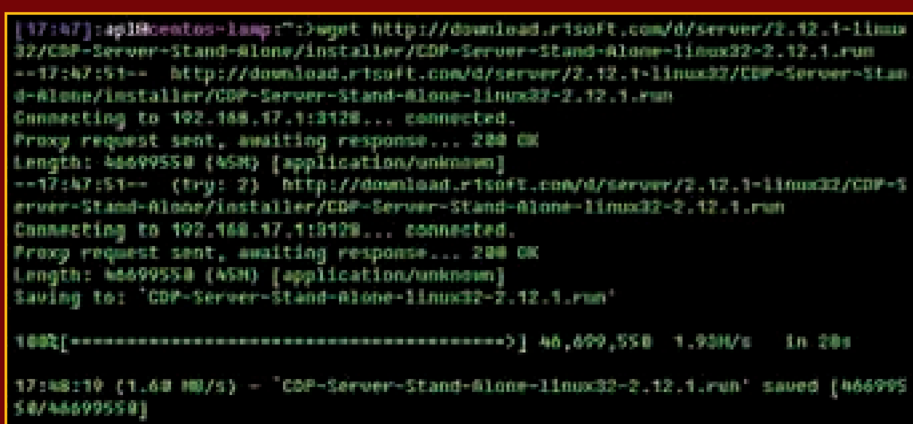
# this website is overloaded, put
all of its traffic in the lower
# priority throughput bucket
<VirtualHost a.b.c.d>
        ServerName piggy
        IPTOS throughput
</VirtualHost>

# this website is special -- and we
override the global threshold
<VirtualHost a.b.c.d>
        ServerName special
        IPTOS lowdelay
        IPTOSthreshold 0 none
</VirtualHost>
```

:: Conclusioni

Come abbiamo visto ci sono diversi modi per risolvere lo stesso problema. Sta a noi scegliere il più consono, sulla base delle nostre esigenze, del bagaglio di competenze e sull'esperienza acquisita. Buon hack a tutti!

Juice



Così appare il pannello di controllo modulo CBAND mentre lo utilizziamo.

La cifratura di Beale



La crittografia, semplice, con una chiave molto, molto lunga

Due su tre sequenze di numeri scritte nel 1822 da un certo Thomas Beale stanno ancora resistendo agli attacchi da parte dei migliori critto analisti del mondo. I tre messaggi sono la chiave per arrivare a un tesoro di valore colossale che sono stati cifrati usando una tecnica, da Beale stesso, che usa come chiave interi testi. Leggenda o verità, la cifratura di Beale ha un algoritmo affascinante e facilmente utilizzabile nella pratica di tutti i giorni e, per questo, vale spenderci un po' di tempo per un approfondimento.

:: Dichiarazione di indipendenza

Il meccanismo della codifica è quasi banale. Viene preso un testo, viene numerata ogni parola e viene fatta una sostituzione delle lettere del testo da cifrare con il numero della parola che ha la corrispondente lettera iniziale. Se il processo viene fatto manualmente, il tempo di codifica e decodifica è comunque accettabile. Se realizzato tramite procedure automatiche, il sistema è piuttosto rapido e permette l'utilizzo di testi anche molto lunghi. Un esempio di applicazione di questo algoritmo è rappresentato dagli stessi crittogrammi di Beale: il secondo è stato decodificato usando il testo della Dichiarazione di Indipendenza. In compenso, gli altri due testi resistono ancora a qualsiasi tipo di analisi. Il

PSEUDOCODICE: IN CIFRA

```
Input testochiaro
Split testochiaro
Dichiarazioni: parsevar, cifrato (= null)
Per ogni testochiaro(x)
    Leggi testo chiave fino alla parola numero parsevar
    parsevar = parsevar +1
    sem aiuscolo(chiave(parsevar))=maiuscolo(chiaro(x))
        cifrato=cifrato&”,”&parsevar
        x++
    parsevar = parsevar +1
fine ciclo
output cifrato
```

problema è che questo algoritmo non ha le debolezze tipiche dei sistemi di cifratura anche moderni. Innanzitutto, la chiave può essere estremamente più lunga del messaggio e ad uso singolo. Questo significa che un'analisi dei numeri che compongono il messaggio codificato non dà alcun risultato di frequenza delle lettere. Allo stesso modo, qualsiasi tentativo di rompere la sicurezza con il brute force è destinato a infrangersi con l'ampia quantità di chiavi possibili: qualsiasi testo, di qualsiasi genere, può essere usato come chiave. Inoltre, l'algoritmo può essere impostato per evitare la ripetizione delle cifre, eliminando completamente qualsiasi appiglio di analisi: il testo cifrato risulta una sequenza di numeri apparentemente casuale. Anche con le variazioni più adatte a evitare i tipici problemi dei testi cifrati, la decodifica può diventare un procedimento mnemonico: basta avere il testo originale. Unico punto che potrebbe rappresentare un problema è l'uso della stessa chiave per più messaggi, che esporrebbe i messaggi stessi a un'analisi comparativa. Un problema che non ci si dovrebbe porre: la codifica di Beale nasce come sistema con chiave "one shoot" e non dovrebbe essere utilizzato per scambi di messaggi basati sulla stessa chiave.

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 191, 122, 43,
234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46,
10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28,
248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2
270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106,
160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353,
320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27,
8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811,
30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50,
154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205,
38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37,
38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84,
125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30,
150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811,
125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302,
246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51,
63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

Il secondo cifrario di Beale. L'unico decodificato. Quasi impossibile decodificare gli altri: l'algoritmo è pressoché inattaccabile con qualsiasi tecnica.

:: Dettagli importanti

Il primo passo da fare è quello di recuperare il testo in chiaro da codificare. Poi basta inserirlo in un array per poter lavorare facilmente con la stringa. A questo punto basterà impiantare un ciclo dal primo all'ultimo carattere per implementare la codifica.
Il secondo passo è quello di recuperare un testo in ingresso, la chiave, collocandola in un'area di memoria che permetta l'accesso numerale alle parole. Per testi brevi è possibile usare un semplice array creato con uno split basato sugli spazi, di una stringa di testo.

Nella realtà, ci dovremmo trovare con una tabella invece di un array: uno split servirà per separare tra loro le parole e un secondo split ci permetterà di dividere le parole in caratteri (se il nostro linguaggio non permette il riferimento diretto ai caratteri che compongono una stringa), così da semplificare al massimo i confronti. In questo modo, il riferimento numerale alla lettera iniziale (e il suo confronto col testo da codificare) sarà basato su semplici cicli.

Effettivamente, questo approccio funziona solo se si usano chiavi di lunghezza ridotta perché le chiavi lunghe possono richiedere una quantità di spazio in memoria troppo elevato e il costo di elaborazione potrebbe essere particolarmente sconveniente. Scegliendo un testo di 3-400 caratteri e una chiave come la Divina Commedia, il costo in memoria della codifica sarebbe inutilmente elevato. Per questo motivo è più conveniente predisporre un parser capace di lavorare direttamente sul file di testo della chiave, così da limitarsi alla trasposizione del testo in chiaro. Allo stesso modo, introducendo l'impossibilità di fare un passo indietro con il parser, avremmo anche la garanzia che le lettere risulteranno codificate in modo univoco, eliminando ogni possibilità di analisi della cifra.

Poi dobbiamo assicurarci che il testo in chiaro non possa essere rintracciato con qualche debolezza intrinseca. In particolare, i numeri del testo in chiaro possono essere difficilmente codificati in un eventuale testo in cifra, a meno che questi non vengano scritti in modo esplicito: "uno" al posto di 1, centoventitremilaquattrocentoventuno al posto di 123.421, e via dicendo. Anzi: usando questo accorgimento, il testo cifrato acquisisce un grado in più di complessità, limitando ulteriormente le possibilità di intercettazione. Per finire occorre anche considerare il problema dello scambio di chiavi: nota difficoltà di qualsiasi sistema di cifratura. In realtà, l'uso di testi disponibili pubblicamente, specialmente se si tratta di libri o riviste pubblicate, permette di suggerire al nostro destinatario la chiave da usare anche se siamo in pubblico. Le ipotesi e le idee sono le più disparate: da innocenti frasi di stato dei social network fino all'ordinazione di libri online.

PSEUDOCODICE: IN CHIARO

```
Input cifrato
Split cifrato(",")
Dichiarazioni: testochiaro (= null)
Per ogni cifrato(x)
    Leggi testo chiave fino alla parola numero cifrato(x)
    testochiaro=testochiaro&c ifrato(x)(1)
    x++
fine ciclo
output testochiaro
```



Prrrrrrronto? Obama?

Il 44° presidente degli USA rappresenta una svolta epocale anche in campo tecnologico: potrà avere un suo telefono personale

Jean Giono, scrittore francese del secolo scorso, diceva del potere che "Chi diviene potente non può più amare". In realtà era un ottimista perché, nella realtà, la persona più potente sulla faccia della Terra non potrebbe nemmeno fare una telefonata per litigare in pace con gli amici. Proprio così: per ragioni di sicurezza nazionale, il presidente degli Stati Uniti d'America non può avere contatti diretti con l'esterno: tutto, anche le telefonate private, deve passare dai suoi collaboratori. Dalla cena col premier russo alla colazione con la moglie, il semplice uso del telefono gli è proibito. Figuriamoci gli SMS, MMS, la posta elettronica, un profilo su Facebook o gli aggiornamenti di stato con Twitter...

:: Libero?

Così può capitare che Barack Obama, eletto grazie a una campagna mediatica che ha visto protagonisti Internet e le nuove tecnologie, convissuto felicemente fino a poco tempo fa con il suo Blackberry, le mail dai sostenitori, i social network e account sparsi un po' dovunque, si accorga improvvisamente che diventare Presidente significa perdere tutte quelle libertà di espressione che hanno fatto il suo punto di forza. Ma non si è potenti se non ci si può permettere di cambiare le regole. Così, dopo un moto di protesta verso la National Security Agency che gli aveva sottratto i suoi gingilli e verso un insieme di regole definite "medioevo tecnologico" dallo stesso Presidente, Barack ha conseguito la sua vittoria. A queste accuse, l'NSA ha risposto consigliando al Presidente l'uso di due telefoni (Sectera Edge di General Dynamics e Guardian di L-3 Communications) ben noti per la sicurezza delle loro comunicazioni e frutto del progetto, condotto dalla stessa NSA, chiamato Secure Mobile Environment Portable Electronic Device. Chiunque abbia visto questi telefoni e li abbia confrontati con qualsiasi Blackberry, però, non può che sorridere: hanno una linea terribile, funzioni a livello embrionale e sono sicurissimi perché i loro sistemi di comunicazione permettono tutto tranne che comunicare agevolmente. La stessa reazione, probabilmente, l'ha avuta anche il Presidente, che non si è dato per vinto. Interessando diret-



Un'ipotesi di come potrebbe essere il Blackberry presidenziale. Visto l'impegno di risorse, quasi certamente le telefonate di Obama saranno tra le più care mai registrate nella storia.

tamente RIM, produttrice dei Blackberry, i maggiori esperti di sicurezza della NSA, laboratori specializzati e altri esperti di fama mondiale, è riuscito a riconquistare il "suo" Blackberry. In realtà non è proprio il suo, visto che RIM ha deciso di sviluppare a tempo record una versione speciale del suo famoso telefono, chiamata "One", per le specifiche esigenze del Presidente e del suo staff. Il motivo di questo lavoro è dovuto al fatto che, per legge, il Presidente degli USA non può avere una corrispondenza realmente privata. Il Presidential Records Act, infatti, prevede che tutti i messaggi inviati dai capi di stato siano inseriti in un registro ufficiale, classificato come segreto nazionale, per essere un giorno resi accessibili al pubblico e agli storici, come già accade oggi per i primi Presidenti USA. Inoltre, una copia di ogni messaggio, anche sotto segreto, può essere richiesta dai giudici. A questo problema legale si somma quello della sicurezza: le normali linee telefoniche, così come i software di tutti i dispositivi di largo consumo, possono essere facilmente hackerati e si teme che qualche pirata possa intercettare la posta di Obama.

:: Via il vecchiume!

La prima battaglia del Presidente USA che più di tutti promette sostanziali novità sociali ed economiche, quindi, è stata quella per riacquisire la propria libertà personale grazie a un compromesso con i rigidi direttori dell'NSA: verrà prodotto un centinaio di telefoni Blackberry One che il Presidente potrà distribuire a collaboratori, parenti e amici fidati e che gli permetterà di restare in contatto, almeno in parte, con il suo network personale. Per ragioni di sicurezza, questi telefoni ingloberanno un algoritmo di cifratura studiato appositamente per rendere sicure le comunicazioni presidenziali. In più, dal punto di vista dei server, è in fase di creazione una versione speciale del BlackBerry Enterprise Server che verrà installata alla Casa Bianca con un mirror al Pentagono. Questo tanto per cominciare, visto che Obama stesso trova assolutamente inconcepibile la richiesta di rinunciare a portare il suo laptop nella Sala Ovale, così come l'impossibilità di tenere contatti diretti, via mail, con qualche suo elettore. Tutte questioni che il Presidente sta affrontando personalmente, tacciando l'NSA e l'intera organizzazione presidenziale di essere arretrati. D'altra parte lo staff della Casa Bianca



L'agenzia nazionale della sicurezza si occupa di spionaggio e controspionaggio. Ultimamente ha molto da fare con i telefonini...

è abituato a cambiare e a darsi da fare per rispettare le volontà e i capricci dei vari Presidenti e delle loro famiglie: i figli di Roosevelt, uno dei presidenti più amati, distrussero il giardino per farne un campo da baseball, usarono i ritratti appesi ai muri come bersagli per il tiro con l'arco, riempirono l'austera White House di animali tra cui un pony, costretto a salire sull'ascensore presidenziale. Alla luce del passato e delle esigenze moderne, la richiesta di Barack Obama di poter continuare la sua vita privata pare ben poca cosa.



Il rinnovamento politico del Presidente USA parte proprio dalle nuove tecnologie: dal sito della Casa Bianca è possibile consultare migliaia di documenti sui temi più disparati, all'insegna della trasparenza assoluta .



Le calcolatrici scientifiche? Possiamo utilizzarle anche per programmarci dei videogiochi

Super Mario nella calcolatrice

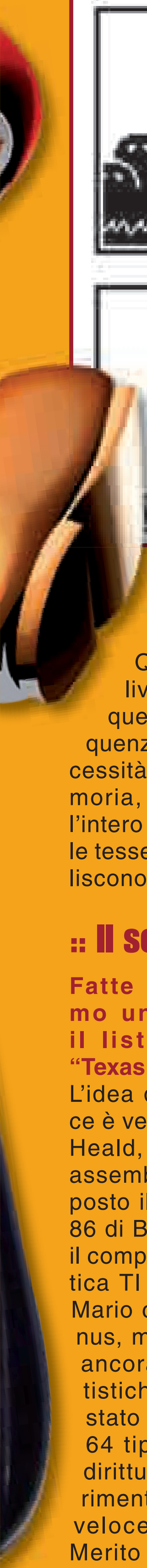


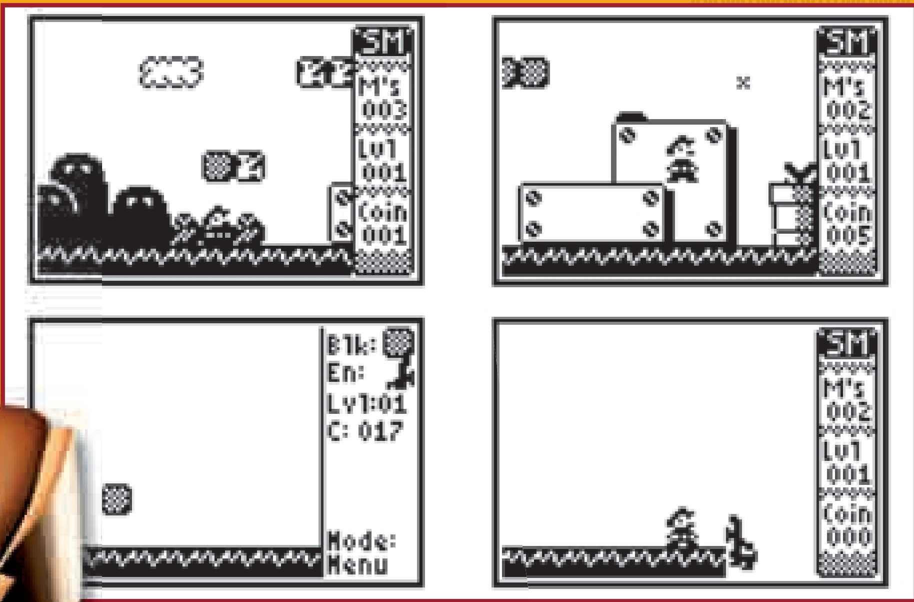
Chi non ha mai usato a una calcolatrice Texas Instruments alzi la mano! I mitici elaboratori tascabili dell'azienda americana rimangono tra i più apprezzati sul mercato, e uno strumento irrinunciabile per quanti hanno a che fare coi calcoli scientifici. Tra i loro punti di forza, almeno nei modelli di fascia media e alta, ci sono un'ampia dotazione di funzioni e un linguaggio di programmazione in grado non solo di gestire il calcolo, ma anche dei comandi grafici elementari e di creare nuove funzioni ad hoc. Questi comandi a basso livello, combinati tra loro, possono dare luogo a immagini statiche o dinamiche anche piuttosto complesse, il cui vero limite è il display della calcolatrice, spesso monocromatico e in bassissima risoluzione. Ma ci si può accontentare di prestazioni simili a quelle dei primi cellulari con cui si poteva giocare a semplici videogames.

:: La forza del linguaggio

Questi limiti tecnici non ci precludono comunque la possibilità di sfruttare il linguaggio di programmazione di una TI-84 (ma la proceedura funziona anche con molti altri modelli simili) per sviluppare un gioco. E nemmeno di quelli semplici: un vero e proprio clone di Super Mario, tanto per essere precisi. Due gli elementi problematici da considerare: il movimento del personaggio e la gestione degli sfondi. Se il primo è risolvibile con poche istruzioni, il secondo richiede qualche premessa tecnica. Super Mario, come buona parte dei videogiochi 2D "a scorrimento", poggia su una struttura a "tile", cioè tessere. In pratica, lo sfondo è costituito da tessere quadrate, intercambiabili tra loro.

le nell'allocare e disallocare continuamente la memoria (che è piuttosto limitata) dell'elaboratore, di modo da non sovraccaricarla di dati e incorrere in spiacevoli e fastidiosi rallentamenti.



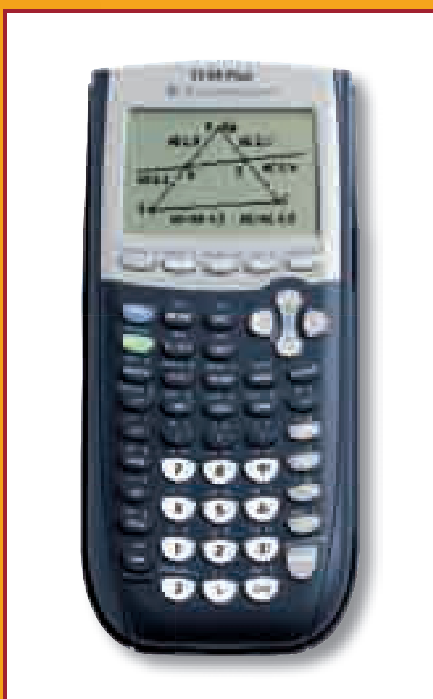


Ecco alcune belle schermate del mitico Super Mario, catturate dalla versione programmata per calcolatrice grafica Texas Instruments.

Quindi, il background di ogni livello è in realtà composto da queste tessere, arrangiate in sequenze diverse a seconda delle necessità. Così si risparmia molta memoria, perché al posto di caricare l'intero sfondo è sufficiente caricare le tessere e le istruzioni che ne stabiliscono l'ordine di visualizzazione.

:: Il segreto? È nel listato

Fatte queste premesse, vediamo un po' di armeggiare con il listato di questa versione "Texas Instruments" di Super Mario. L'idea di un'edizione per calcolatrice è venuta all'abilissimo coder Sam Heald, che sfruttando il linguaggio assembly della sua TI-83, ha riproposto il concept dell'originale Mario 86 di Bill Nagel, sfruttandone anche il comparto grafico. Di fatto, sulla mitica TI possiamo ricreare un Super Mario completo di tutto: nemici, bonus, monete, trappole e molto altro ancora. Per chi di noi ama le statistiche, la versione TI vanta, allo stato attuale, 13 diversi avversari, 64 tipi di tile diverse (alcune addirittura animate) e fondali a scorrimento veloce. E quando diciamo veloce, intendiamo molto veloce. Merito di una programmazione sopraffina, che può essere apprezzata dai veri intenditori del buon codice grazie ai numerosi commenti che arricchiscono il listato del programma. Per chi conosce l'assembly, e in particolare quello delle macchine Texas Instruments, il consiglio è dunque quello di osservare la cura maniaca-



Anche la moderna TI-84 beneficia del videogioco di Super Mario!

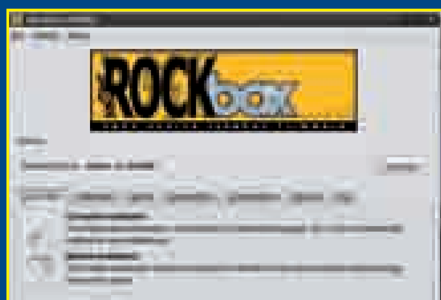
:: Struttura del programma

La struttura di base del codice di Super Mario TI si compone del programma principale, nel file mario.8xp, che contiene tutta la grafica e i livelli, e del file aggiuntivo nagel.8xp che contiene un livello in più a opera di Bill Nagel. Il file del progetto, scaricabile da www.ticalc.org/pub/83plus/asm/games/ion/arcade/mario83p.zip, include però altro materiale, peraltro davvero sfizioso. Su tutto un potente ed efficiente level editor, nel file Medit.8xp. Se utilizziamo una TI-83, i file da considerare sono invece quelli con estensione 83p, presenti anch'essi nel file ZIP. Qui dentro, come anticipato, troviamo anche il sorgente del programma assembly, nel file mario.asm (mentre per l'editor il file di riferimento è medit.asm).
Se abbiamo voglia di trasformare subito la nostra calcolatrice Texas Instruments in una console da gioco, non ci resta che installare Super Mario. Per farlo, però, dobbiamo prima installare Ion. SI tratta della shell per il linguaggio assembly delle TI-83 e TI-84. La scarichiamo da http://joewing.net/programs/calc/ti83/ion.zip. Fatto questo,estraiamo i file dall'archivio e, a seconda della calcolatrice utilizzata, inviamogli ion.83g o ion.8xg. Una volta installato Ion, passiamo pure a Super Mario. Inviamo prima di tutto il file principale del programma, poi il livello aggiuntivo e, infine, il level editor. Terminata l'installazione, passiamo alla partita vera e propria: controlliamo il nostor amato Mario con la freccia destra e sinistra, saltiamo col pulsante 2ND, speriamo le firewall con ALPHA e infine, mettiamo in pausa con MODE e usciamo con CLEAR. Insomma, con un po' di fatica possiamo divertirci alla grande anche con una semplice calcolatrice, solitamente bistrattata in favore del fratello maggiore, il PC. Eppure, con una buona dose di passione per l'hacking, visto che si può fare?

L'iPod diventa Rock

Come si installa RockBox un firmware alternativo per iPod e altri player MP3

Il più grande limite dei player MP3 risiede nei vincoli imposti dai produttori. Fra questi, Apple limita fortemente l'utilizzo dei suoi iPod, legandoli al programma iTunes; oltretutto, non è possibile nemmeno sincronizzare il proprio iPod su un altro computer con iTunes, per via delle politiche restrittive legate al copyright dei brani. Ovviamente, se il vostro iPod è formattato in standard Windows e non Apple, si può già aggirare il problema mostrando gli elementi nascosti e puntando alla directory iPod Control, ma si può fare qualcosa in più. RockBox nasce con l'intento di estendere le possibilità dei player MP3; nel caso dei player Apple, si può installare sugli iPod dalla prima alla quinta generazione (5.5 per essere precisi), iPod mini e iPod nano prima generazione, (gli altri iPod non sono supportati). Per quanto riguarda le altre marche troviamo modelli di Toshiba, Sandisk, iRiver, Cowon, Archos e Olympus (www.rockbox.org/twiki/bin/view/Main/ReleaseNotes32#Supported_players). La lista delle caratteristiche aggiuntive rese possibili grazie a RockBox è davvero lunga, ma vi elenchiamo le più salienti: lettura di codec aggiuntivi come Shorten, Flac, Ogg/Vorbis, MPEG Audio, MPC, MonkeyAudio; equalizzatore parametrico programmabile a 5 bande; estensione/compressione del panorama sonoro; eliminazione del limitatore sul volume di uscita; crossfading; riproduzione dei file MPEG, struttura a plugin estensibile; supporto per i comandi vocali; skin personalizzate e molto altro ancora.



Il programma RbutilQT permette di installare RockBox in pochi passaggi.



:: Installazione

Dal sito www.rockbox.org si può scaricare la release corrente, la 3.2, che dopo diversi anni di sviluppo è finalmente giunta a una versione stabile. Essendo un progetto Open Source, è possibile contribuire: nella Wiki si trovano tutte le informazioni del caso all'indirizzo www.rockbox.org/twiki/bin/view/Main/DevelopmentGuide.
Per quanto riguarda l'installazione, ne illustreremo i passaggi utilizzando l'eseguibile per Linux. Scaricatelo in formato binario adatto alla vostra piattaforma (32 o 64 bit), scompattatelo e quindi aprite una finestra di terminale. Entrate nella directory che avete appena scompattato (rbutilqt-v1.2.1) e lanciate l'eseguibile rbutilqt come utente root. Potete usare il comando sudo oppure accedere direttamente alla shell di root con il comando su. Ricordatevi che, essendo un programma non installato nel vostro sistema, per lanciarlo dovrete specificare tutto il percorso, altrimenti vi verrà restituito l'errore "comando non trovato". Prima di avviare il programma, assicuratevi che il vostro player sia collegato e visibile al sistema; inoltre, nel caso degli iPod, è necessario che siano stati formattati con file system FAT32 e non HFS. Se così non è, bisogna prima resettarlo e preparlo da una macchina Windows con iTunes. Ricordatevi che la reimpostazione cancella tutta la vostra libreria musicale nell'iPod, quindi assicuratevi di averne una copia sul computer. Avviata l'applicazione, dovrebbe riconoscere la periferica collegata e impostarla senza problemi. In caso contrario, cliccate sull'icona Change e puntate al vostro dispositivo, specificando anche il modello. Ora, un ultimo click su Complete Installation avvia la procedura automatica e, seguendo i pochi passaggi richiesti terminerete l'installazione di RockBox, completo di temi extra, font e giochi. Potete ora creare una directory sull'Ipod nella quale memorizzare tutti i file musicali. Al primo tentativo di riproduzione, RockBox vi avvertirà che serve un file di database, quindi lanciate la procedura per crearlo. RockBox non fa distinzioni di percorsi e cerca i file di sua competenza in qualsiasi directory presente sul dispositivo. Se volete escludere una directory dalla scansione, create un file vuoto chiamato database.ignore e sistematelo nella directory da escludere. Questo va fatto anche per le sottodirectory, quindi potreste avere una directory radice ignorata, ma le sue sottodirectory indicizzate. RockBox permette moltissime personalizzazioni: non vi resta quindi che esplorare tutti i menu e iniziare a usare il vostro player MP3 in una maniera del tutto nuova!

meksONE



I player MP3 supportati Sono moltissimi. Gli iPod, soprattutto i modelli Photo o Video, diventano davvero interessanti con RockBox.





Auditor Security Collection



La distribuzione Linux utilizzata anche dall'FBI

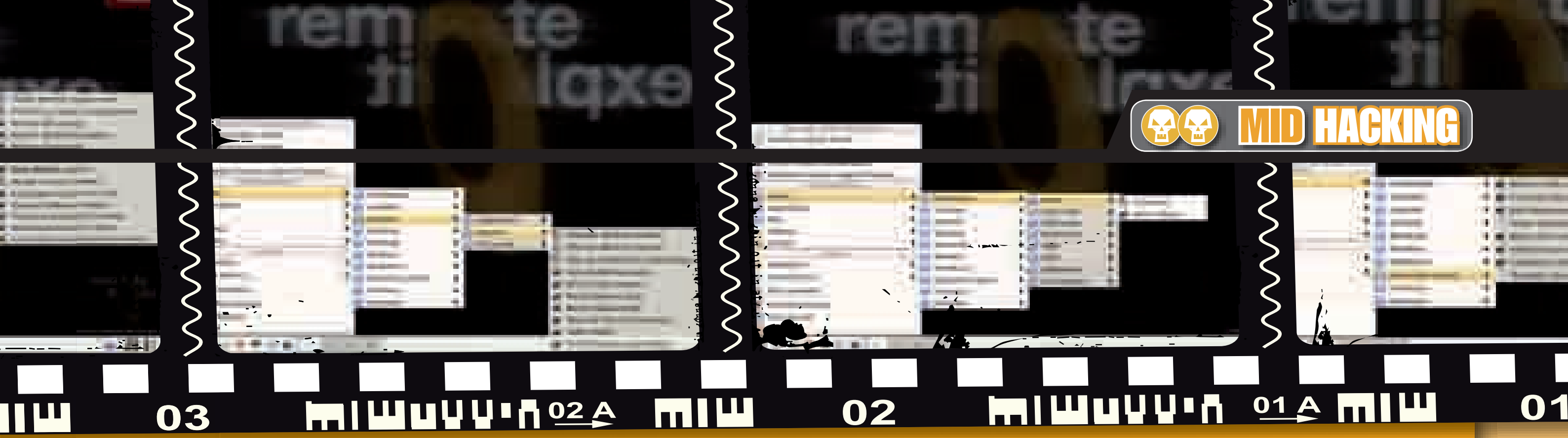
Abbiamo parlato pochi numeri fa del rilascio di BackTrack 4 Beta e, mentre attendiamo l'uscita della release finale, approfondiamo la conoscenza di Auditor Security Collection, la distribuzione di cui BackTrack è figlia. Auditor è un sistema live che inizialmente era basato su Knoppix, mentre a partire dal 2005 è stato basato su Kanotix per via di diverse migliorie introdotte. Il vantaggio di essere live permette di poterlo provare su qualunque macchina a disposizione senza intaccarne la configurazione, soprattutto per gli addetti ai lavori, che possono trovarsi nella situazione in cui va verificata la sicurezza da un nodo della rete durante un sopralluogo. Nelle ultime versioni rilasciate (già con il logo di www.remote-exploit.org) comunque è stato inserito uno script grafico costruito per effettuare l'installazione stabile su hard disk che, in modo semplificato permette di passare facilmente dalla versione live in sola lettura a quella standard completamente personalizzabile.

:: Come si presenta Auditor

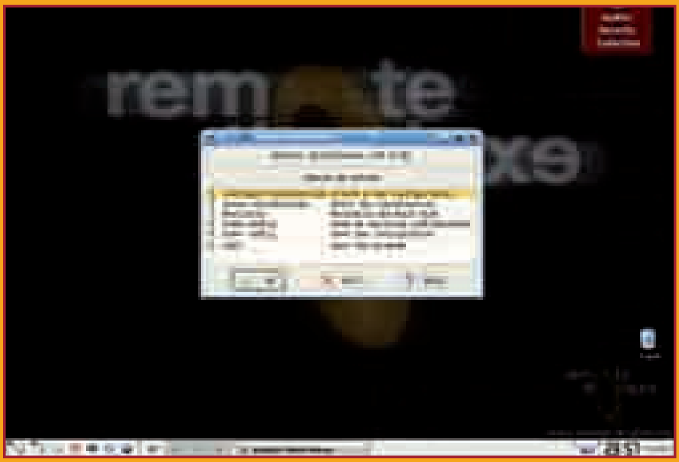
Auditor si presenta come un arsenale da guerra per la sicurezza informatica con svariate applicazioni preinstallate dedicate a test di penetrazione di LAN/WLAN e tool per forzare dispositivi con bluetooth. Per superare alcuni problemi di compatibilità con i dispositivi WiFi di Intel (che nel 2006 non erano stati ancora risolti) l'ultima release di Auditor realizzata è stata rilasciata in due versioni: con supporto IPW2100 (Auditor-200605-02-ipw2100.iso) e senza tale supporto (Auditor-200605-02-no-ipw2100.iso). Nel caso occorra il driver IPW2200 è sconsigliato usare la versione con il driver IPW2100 integrato a meno di aggiornare manualmente il kernel presente di Linux (2.6.11) e superare queste limitazioni. Auditor offre un ambiente standardizzato



Caricamento dell'interfaccia grafica di Auditor. Al boot di sistema è possibile selezionare poche modalità grafiche, tra cui quelle fail-safe in caso si avessero problemi di visualizzazione.



e stabile che ne facilita l'apprendimento e l'utilizzo. È stata prestata particolare attenzione per renderlo il più possibile user-friendly, pur mantenendo la potenza degli strumenti, a partire dalla loro classificazione che ricalca le fasi di un controllo di sicurezza: foot-printing, analysis, scanning, wireless, brute forcing, cracking. Sono presenti anche svariate applicazioni di uso comune (immancabile Firefox, ma anche altri browser) che facilitano l'attività di studio e l'utilizzo della distribuzione, ma il punto di forza è rappresentato chiaramente dai tool specifici per i test di sicurezza, alcuni dei quali addirittura riscritti o convertiti da altri sistemi e piattaforme allo scopo di averne il maggior numero possibile in un unico CD-ROM. Per esempio, alcuni tool, come Wellenreiter e Kismet, sono stati equipaggiati con un'identificazione automatica dell'hardware per evitare irritanti o noiose configurazioni delle schede wireless.



Lo script di installazione è spartano, ma funzionale. Sostanzialmente si può ripartizionare l'hard-disk e avviare l'installazione.

:: Dove si può scaricare Auditor

Dove è possibile scaricare Auditor? Sembra una domanda scontata, ma in realtà non è facile trovare siti che permettono il download delle ISO di questa distribuzione, molto probabilmente a causa del fatto che parliamo di una distribuzione non più supportata, ma è anche possibile che dipenda dalla natura al limite della legalità del prodotto. Lo stesso team che lo ha sviluppato, Remote-Exploit, non lo visualizza più sul proprio sito. Un mirror che in questo momento le rende disponibile è http://ftp.dkuug.dk/security/Auditor.

:: Considerazioni

Auditor rappresenta uno strumento didattico che permette di valutare seriamente la sicurezza di un sistema o di una rete da molti punti di vista. Il suo utilizzo è chiaramente limitato dalle competenze dell'uente, ma l'orientamento che viene dato a livello di interfaccia stimola a provare nuove possibilità e quindi a imparare a usare strumenti più complessi. Tanto per citare un esempio, l'insostituibile Nmap viene indicato tra i tool dedicati all'identificazione di un sistema operativo e può essere lanciato da menu con questo solo scopo, ma sappiamo bene che le sue potenzialità vanno molto oltre. Pur apparentemente superato dalle versioni di BackTrack, rappresenta a mio parere un ottimo punto di partenza per chi voglia approfondire le tematiche di sicurezza e valutare quindi le nuove distribuzioni in base ai criteri di chiarezza e funzionalità che erano stati inseriti in Auditor.

Massimiliano Brasile

NESSUS C'E'

Gli strumenti inseriti nell'ultima release di Auditor. Compare anche Nessus, stranamente escluso da BT4.

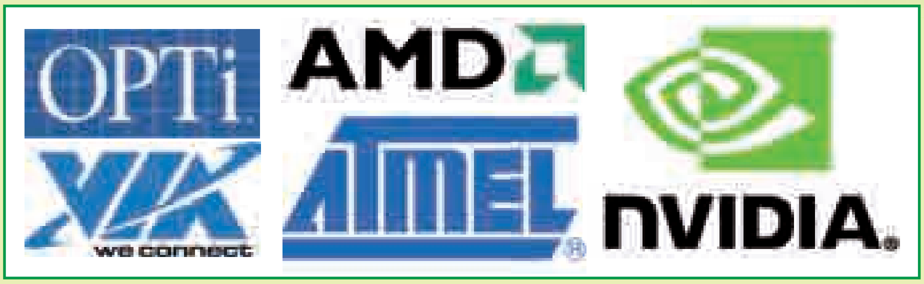
- **proxychains 1-8-1** (per uno scanning via proxy più facile)
- **yersinia-0.5.4**
- **kismet-logfile-viewer klv.pl** e **klc.pl**
- **ntp** fingerprinting tool
- **tftp** bruteforce tool
- **snmp fuzzer**
- **cisco torch 0.4b**
- **unicornscan 0.4.2**
- **packit**
- **sendip**
- **nasl 2.2.4**
- **tcpick**
- **cryptcat**
- **amap** versione **4.8**
- **tcpsplit**
- **Ethereal version 10.11**
- **ettercap-ng-0.72** con modifica a **etter.conf**
- **snmp tools** sostituisce **tinysnmp**
- **vnc2swf /usr/X11R6/bin/recordwin** e **vnc2swf**
- **edit_vnc2swf.py**
- **edit_mp3.py**
- **wpa-supplicatiant 0.3.8**
- **hostapd-utils 0.3.7**
- **ssldump**
- **fragrouter**
- **Metasploit 2.4** con tutti gli aggiornamenti
- **airsnarf,** ma per il momento senza menu
- **fakeap** a **/opt/Auditor** ma per il momento senza menu bisogna scrivere uno shell script
- **dsniff 2.4b1-10**
- **nessus plugins** aggiornato
- **exploit tree** aggiornato
- **Snort 2.3.2-5**
- **Bleeding-edge rules** per **snort**
- **aircrack** nuovo
- **airsnort** nuovo

Ci sono aziende che hanno trovato un business molto redditizio: il risarcimento danni per la violazione di brevetto. Ma sono veri brevetti?



Il valore di un'idea

Doveva succedere, ed è successo. Più o meno settemila anni dopo, la Mela è stata morsicata ancora. Solo che questa volta a peccare è stata proprio lei, la grande Mela di Steve Jobs. La novella Eva è la californiana Opti Incorporated con sede a Palo Alto, che è riuscita a staccare un morso da 19 milioni di dollari. È vero che la casa di Cupertino ha messo a bilancio 30 miliardi di dollari di utile, ma 19 milioni sono pur sempre un bel mangiare! L'oggetto del contendere è un brevetto registrato e regolarmente riconosciuto, il 6,405,291 del 2002, ed è incentrato sul cosiddetto Predictiv snooping of cache memory for master-initiated accesses, che in italiano, e soprattutto in non legalese, identifica una tecnologia per migliorare le performance del trasferimento dati tra processore, memoria cache e altre unità di processing. Apple ha ammesso candidamente di aver utilizzato questa tecnologia, talmente ovvia che chiunque avrebbe potuto concepirla (e che nessuno si sarebbe mai immaginato fosse coperta da brevetto), e ha incentrato la sua difesa su questo presupposto… perdendo miseramente un dibattimento durato otto giorni. I legali di Apple, subodorata l'imminente bastonata, avevano stimato in 270 mila dollari l'equo scotto da pagare per aver violato il brevetto. Evidentemente la Corte Distrettuale Orientale del Texas di Marshall, chiamata anche Patent Lawsuit Valley avendo trattato 236 cause



Tra le vittime illustri di Opti Incorporated figurano nVidia e AMD.

sullo stesso tema nel solo 2006 (di cui il 78% vinte dai querelanti contro il 59% della media nazionale), è stata di ben altro avviso e la sentenza è arrivata puntuale come una cambiale: Apple ha sbagliato ed è giusto che debba pagare una "ragionevole royalty per la violazione".

:: Vittime illustri

Così come aveva dovuto pagare, nel 2006, anche nVidia: stesso querelante, stesso brevetto aggirato, stessa Corte Federale. All'epoca l'ammenda ammontava a 750 mila dollari a trimestre per tre anni, 9 milioni di dollari in tutto. E prima ancora sotto le grinfie della Opti e degli sceriffi del Texas era capitata AMD: l'iter era stato lo stesso, il risultato anche e le prossime vittime annunciate della mietitrice di Palo Alto saranno Standard Microsystems, Atmel, Renesas, Broadcom, VIA, Silicon Storage e ancora AMD, ma questa volta per supposta violazione dei brevetti 5,944,807 e 6,098,141 relativi al Compact ISA (CISA), un'interfaccia di I/O compatibile con il bus Industry Standard Architecture (l'ISA, appunto) di IBM. Questa tecnologia viene utilizzata nelle memorie flash, nei controller embedded (audio, USB, IDE, eccetera) e nei TPM (Trusted Platform Module). La Opti Incorporated, come migliaia di altre aziende in tutto il mondo, vive con i proventi delle cause vinte per violazione di brevetto. Fino al 2003 si occupava di semiconduttori, progettava e produceva componenti, ma a causa della prima grande crisi del settore ha ceduto l'intero asset aziendale alla Opti Technologies per evitare il fallimento e l'unico impiegato superstite si occupa ufficialmente di vendere la proprietà intellettuale della società. Di fatto, la Opti, come tante altre società nella sua condizione, vive di cause. Non produce né beni né servizi, non ha valore aggiunto ma ha avuto la lungimiranza di registrare in tempi non sospetti brevetti su ovvietà e vive di questo. Possibile? Possibilissimo. Il fantastico mondo del brevetto lo permette. È un po' come se brevettassimo la "tecnologia" necessaria per far bollire l'acqua, e citassimo in giudizio chiunque si faccia una pasta. Vuoi l'uovo sodo? Pagami i diritti, la proprietà intellettuale dell'acqua calda è mia. Ti concedo la doccia tiepida perché quello è un altro meccanismo, non ci vuole il pentolino. Per adesso. Non conta più chi è il più bravo a realizzare qualcosa e a offrirlo a un prezzo vantaggioso, conta chi ci ha pensato prima o, peggio, chi è il più veloce nel registrarne l'idea, o chi ha i denari per farlo.

:: Circoli viziosi

Siamo al paradosso, ma senza interventi legislativi per regolare (e possibilmente eliminare) il concetto di brevetto, lo scenario potrebbe non discostarsi troppo dalla tassa sull'acqua calda. Il principio di pagare per l'utilizzo di un'idea, tanto più se ovvia, uccide la concorrenza. Congela l'inventiva. Paralizza il progresso. E porta alla chiusura, all'impoverimento tecnologico, nel nostro caso, ma allargando a macchia d'olio il concetto, anche all'impoverimento culturale e sociale. Ed è quello che sta succedendo oggi. Crisi economica globale? Sì, esiste, ma quella più grave è la crisi di idee: in un momento in cui non ce ne sono di nuove, quelle utilizzabili sono chiuse nei cassetti di chi le ha bollate con un certificato di proprietà e vuole farsi pagare per concederne l'utilizzo. Come sosteniamo da sempre le idee devono nascere, evolversi, migliorarsi, mutare di forma e di sostanza per aiutare a trarre un beneficio e per farlo devono necessariamente essere libere da qualsiasi vincolo, specialmente se economico. Ma le cose forse potrebbero cambiare: un primo, timido, passo in avanti è stato fatto dal Comitato del Senato degli Stati Uniti, che si sta occupando di emendare delle norme di legge specifiche per rivedere il metodo di valutazione dei danni che è stato utilizzato fino a oggi. In pratica il giudice avrà la facoltà di decidere se il brevetto violato è fondamentale o secondario, per differenziare le sanzioni da infliggere in "light" (in caso di brevetto secondario come quello aggirato da Apple), o "strong", nel caso di brevetti per principi tecnologici evoluti. Attualmente la valutazione del danno subito da una società avviene calcolando il valore di mercato del prodotto che ha utilizzato il brevetto violato e spesso la violazione di un brevetto comporta l'aggiramento di decine di altri brevetti.



Il brevetto violato riguarda il trasferimento dati tra CPU e memoria.

Ma il lavoro dei senatori va oltre: il querelante non potrà più scegliere dove intentare una causa, il tribunale sarà assegnato d'ufficio. Questo per evitare di avviare processi in giurisdizioni favorevoli, propense a difendere il brevetto, come quella di Marshall in Texas appunto! Sono solo primi timidi passi, siamo ancora lontani dall'affrontare la questione della legittimità del concetto di brevetto, però qualcosa si sta muovendo. Intanto la taiwanese Elan Microelectronics ha fatto causa ad Apple per la violazione di un brevetto relativo agli schermi touch screen...